



Wireless Broadband Router

A02-RB-W54



MANUALE COMPLETO

A02-RB-W54(V1.1) _MI01

Where solutions begin



Where solutions begin



INDICE

CAPITOLO 1: INTRODUZIONE AL PRODOTTO	1
1.1 Panoramica del Wireless Broadband Router	1
1.2 Contenuto della confezione	1
1.3 Caratteristiche tecniche	2
1.4 Requisiti di Sistema per la configurazione	3
1.5 Schema di installazione del Wireless Broadband Router	5
1.6 Considerazioni sull'Installazione	5
CAPITOLO 2: USO DEL WIRELESS BROADBAND ROUTER	7
2.1 Precauzioni nell'uso del Wireless Broadband Router	7
2.2 I LED frontali	8
2.3 Le porte posteriori	9
2.4 Cablaggio	10
CAPITOLO 3: CONFIGURAZIONE	11
3.1 Prima di iniziare	11
3.1.1 Configurazione del PC in Windows 95/98/ME	12
3.1.2 Configurazione del PC in Windows NT4.0	13
3.1.3 Configurazione del PC in Windows 2000	14
3.1.4 Configurazione del PC in Windows XP	15
3.1.5 Configurazione in ambiente MAC	16
3.1.6 Verifica della Configurazione	16
3.2 Settaggi di Default	17
3.2.1 Password	17
3.2.2 Porte LAN e WLAN	17
3.3 Configurazione tramite Browser	18
3.3.1 Setup Wizard	19
3.3.2 Navigare nell'interfaccia Web di Configurazione	31
3.4 WAN	32
3.4.1 Connection Type	32
3.4.2 Dynamic DNS	39
3.5 Wireless	40
3.5.1 Basic	40
3.5.2 Security	41



3.5.3 Advanced	44
3.6 LAN	45
3.6.1 Basic	45
3.6.2 DHCP	46
3.7 Access Control	49
3.7.1 Filter	49
3.7.1.2 MAC Filter	50
3.7.1.3 IP Filter	52
3.7.1.4 URL Blocking	53
3.7.1.5 Domain Blocking	54
3.7.1.6 Protocol Filter	55
3.7.2 Virtual Server	56
3.7.3 Special AP	61
3.7.4 DMZ	62
3.7.5 Firewall Rule	64
3.8 System	69
3.8.1 Password	69
3.8.2 Time	71
3.8.3 Device Information	72
3.8.4 Log	74
3.8.5 Log Settings	75
3.8.6 Statistics	77
3.8.7 Restart	77
3.8.8 Firmware	78
3.8.9 Configuration	79
3.8.10 UPnP	80
3.8.11 Ping Test	80
3.8.12 Remote Management	81
APPENDICE A: RISOLUZIONE DEI PROBLEMI	83
A.1 LEDs	83
A.1.1 LED Power	83
A.1.2 LED LAN	83
A.1.3 LED WLAN	84
A.2 Configurazione WEB	84
A.3 Login con Username e Password	84
A.4 Amministrazione remota	85
A.5 Domande Generali	86



APPENDICE B: COME AVVIENE LA COMUNICAZIONE WIRELESS	95
APPENDICE C: SICUREZZA NEL WIRELESS	98
APPENDICE D: ACCESS POINT O ROUTER	100
APPENDICE E: COPERTURA	102
APPENDICE F: CONSIDERAZIONI SULLA SALUTE	105
APPENDICE G: PACKET FILTER	107
APPENDICE H: DYNAMIC DNS	111
APPENDICE I: REGOLAMENTAZIONE	113
APPENDICE J: CARATTERISTICHE TECNICHE	114
APPENDICE K: SUPPORTO OFFERTO	115



Wireless Broadband Router

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land spa che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land spa. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

Restrizioni di responsabilità CE/EMC

Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.

Se il prodotto fosse utilizzato con un PC non certificato, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l'utilizzatore è responsabile della "compliance" con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.

CE Mark Warning

Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

ATTENZIONE

Lasciare almeno 30cm di distanza tra le antenne del dispositivo e l'utilizzatore.



Dichiarazione di Conformità

Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-1, EN 301 489-17(compatibilità elettromagnetica) ed EN 60950(sicurezza). Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:

Francia:

Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per informazioni ulteriori consultare www.art-telecom.fr.

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestici genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.

Italia:

Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: www.comunicazioni.it.

CAPITOLO 1: Introduzione al prodotto

Questo manuale è stato pensato per un utilizzo avanzato Wireless Broadband Router, per questo sono stati trattati con dovizia di particolari una moltitudine di argomenti che potrebbero, almeno inizialmente, scoraggiare alcuni utenti. Per una configurazione rapida è comunque disponibile una Guida all'Installazione presente sia su CD Rom che su supporto cartaceo a corredo del prodotto.

1.1 Panoramica del Wireless Broadband Router

Il Wireless Broadband Router consente una completa mobilità mantenendo sempre una continua connessione.

Semplice da installare, veloce e flessibile, permette di decidere in quale ambiente lavorare con il portatile o PC fisso, attraverso un accesso wireless. E' finalmente possibile estendere l'attuale rete LAN senza la preoccupazione di cavi ingombranti.

Il chipset Atheros garantisce inoltre il pieno supporto hardware, senza nessuna degradazione di performance, degli standard di sicurezza più recenti, come il Wi-Fi Protected Access (WPA/WPA2) e IEEE 802.11i.

Il Wireless Broadband Router dispone di un sofisticato firewall integrato che include anche funzionalità avanzate di ispezione dei pacchetti, anti intrusione, URL Blocking e Domain Blocking.

La rete wireless sarà finalmente scattante ed a prova di hacker.

Tramite la comoda interfaccia Web è possibile accedere velocemente e facilmente a tutte le funzioni offerte dal Wireless Broadband Router che, grazie al client Dynamic DNS integrato, può essere configurato anche da remoto indipendentemente dal tipo di abbonamento ADSL utilizzato.

1.2 Contenuto della confezione

Una volta aperta la confezione in cartone, dovrebbero essere presenti i seguenti componenti:

- Wireless Broadband Router
- CD Rom contenente il manuale (Italiano, Inglese e Francese) e la guida rapida
- Guida di Quick Start (Italiano, Inglese, Francese e Spagnolo) stampata
- Alimentatore AC-DC (7.5V DC @ 1A)
- 1 Antenna da 2.2 dBi (R-SMA)
- Tagliando di Garanzia

Qualora mancasse uno qualsiasi di questi componenti rivolgersi immediatamente al rivenditore.

1.3 Caratteristiche tecniche

Caratteristiche offerte dal Wireless Broadband Router:

- **Conforme alle specifiche IEEE 802.11g e IEEE 802.11b:** E' possibile utilizzare tutti gli apparati esistenti compatibili col protocollo IEEE802.11g e/o IEEE802.11b.
- **Funzionalità Wi-Fi Protected Access (WPA/WPA2) e WEP encryption:** E' possibile utilizzare il massimo livello di sicurezza senza nessuna degradazione di performance.
- **2 Antenne:** Un'antenna esterna sostituibile ed orientabile per una migliore ricezione (grazie alla diversità) ed una più estesa copertura ed una interna fissa.
- **5 porte Fast Ethernet:** tutte e 5 le porte integrano la funzionalità MDI-II/MDI-X e pertanto possono funzionare indipendentemente tanto con cavi dritti che incrociati. Grazie a questa funzionalità è sufficiente collegare i dispositivi, penserà il dispositivo ad adeguarsi al tipo di cavo.
- **Quick Installation Wizard:** Grazie al supporto di un'interfaccia di configurazione via WEB, l'apparato risulta essere facilmente configurabile. E' disponibile inoltre una comodissima Wizard che guida passo passo l'utente alla configurazione del Router.
- **Network Address Translation (NAT):** Consente a diversi utenti di accedere alle risorse esterne, come Internet, simultaneamente attraverso un indirizzo IP singolo. Sono inoltre supportate direttamente : ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting e altro.
- **Firewall:** Supporta un SOHO firewall con tecnologia NAT. Automaticamente scopre e blocca l'attacco di tipo Denial of Service (DoS) attack. Il Wireless Broadband Router è fornito anche di un filtro di tipo URL Blocking e Domain Blocking per una maggiore profondità di filtraggio dei pericoli derivanti da Internet. L'attacco dell'hacker è registrato e conservato in un'area protetta.
- **Packet Filtering:** Non solo filtra i pacchetti in base all'indirizzo IP ma anche in base alla porta usata (dunque il tipo di pacchetti TCP/UDP/ICMP). Questo può migliorare le prestazioni nella Lan oltre che a provvedere ad un controllo di alto livello.
- **Dynamic Domain Name System (DDNS):** Il Client Dynamic DNS permette di associare ad un indirizzo IP dinamico (che vi viene di volta in volta assegnato dal server dell'ISP) un nome statico (host-name). E' necessario, per utilizzare il servizio, effettuare una registrazione gratuita per esempio su <http://www.dyndns.org/>. Sono supportati differenti servizi DDNS (fare riferimento all'appendice H).

- **Virtual Server:** L'utente può specificare alcuni servizi da rendere disponibili per utenti esterni. Il Wireless Broadband Router può riconoscere le richieste entranti di questi servizi e rigirarle all'opportuno PC della Lan. E' possibile, per esempio, assegnare una data funzione ad un PC della Lan (come server Web) e renderlo disponibile in Internet (tramite l'unico IP statico disponibile). Dall'esterno è così possibile accedere al server Web che resta comunque protetto dal NAT. Grazie all'uso della tecnologia DDNS non è necessario che il Router abbia un abbonamento con IP fisso.
- **Dynamic Host Control Protocol (DHCP) client and server:** Lato WAN, il dispositivo può, grazie al DHCP client, prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della Lan.
- **Mac Filtering:** Tramite questa funzionalità è possibile filtrare ulteriormente il traffico limitando l'accesso in base all'indirizzo MAC degli apparati di rete. Sarà possibile bloccare l'accesso ad una lista di MAC Address.
- **UPnP:** Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di configurarsi automaticamente senza l'intervento dell'utente. Chiunque dunque sarà in grado, senza conoscere complicati concetti, di godere pienamente dei vantaggi del NAT e contemporaneamente utilizzare le più comuni applicazioni Internet senza il minimo problema.
- **Configurabile (GUI) via Web:** La gestione e la configurazione sono possibili via interfaccia grafica (browser).
- **Firmware Upgrade:** E' possibile effettuare l'upgrade del firmware tramite interfaccia WEB.
- **Atheros XR® (eXtended Range) Technology:** Il pieno supporto della tecnologia Atheros XR® (Extended Range) permette una copertura più uniforme (con una diminuzione significativa delle zone morte) e un incremento del raggio di azione del prodotto di quasi 2 volte in ambienti Outdoor.

1.4 Requisiti di Sistema per la configurazione

Prima di iniziare l'installazione del dispositivo controllare i seguenti requisiti:

- Un Computer con un qualsiasi Sistema Operativo e lo stack TCP/IP correttamente installato
- Internet Explorer V6.0 o successivi (Netscape V6.0 o successivi)
- CDRom



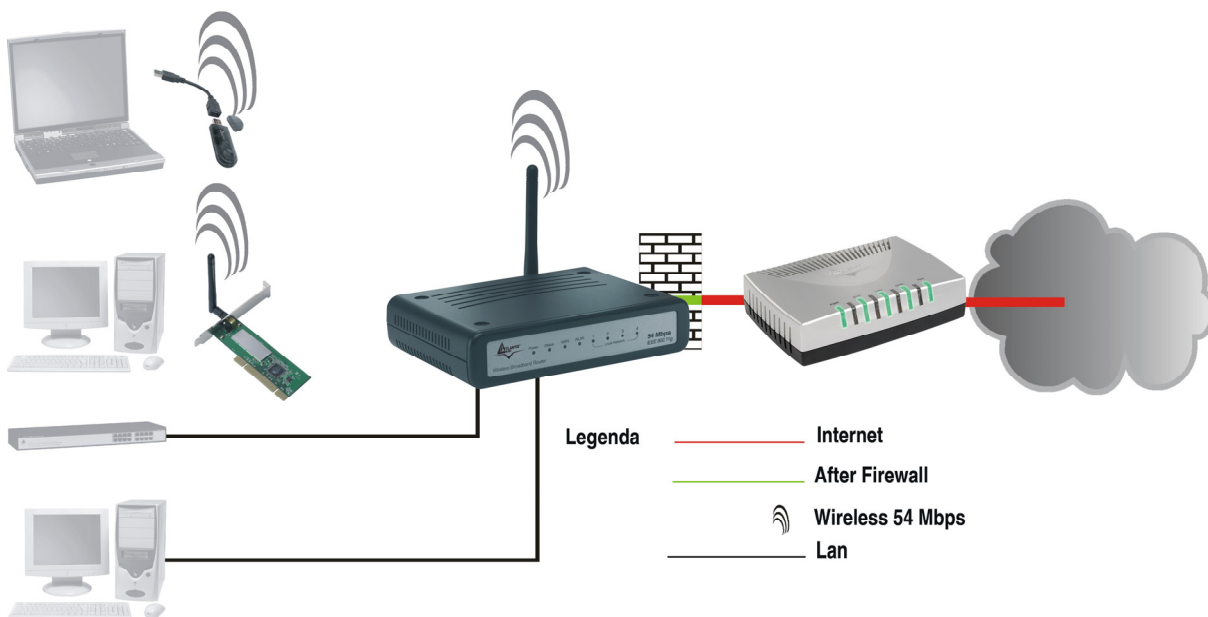
Wireless Broadband Router

1.5 Schema di installazione del Wireless Broadband Router

Seguire i seguenti punti per effettuare il cablaggio del dispositivo:

- Il Wireless Broadband Router può essere collegato, tramite la porta RJ45 (LAN) alla LAN e tramite la porta WAN al Router/Modem ADSL o al dispositivo responsabile della connettività.
- Collegare l'alimentatore **AC-DC (1A /7.5V)** alla rete elettrica e all'apposito attacco (**DC IN**) situato nel pannello posteriore.

E' possibile vedere in figura un esempio di cablaggio di una rete con diversi PC.



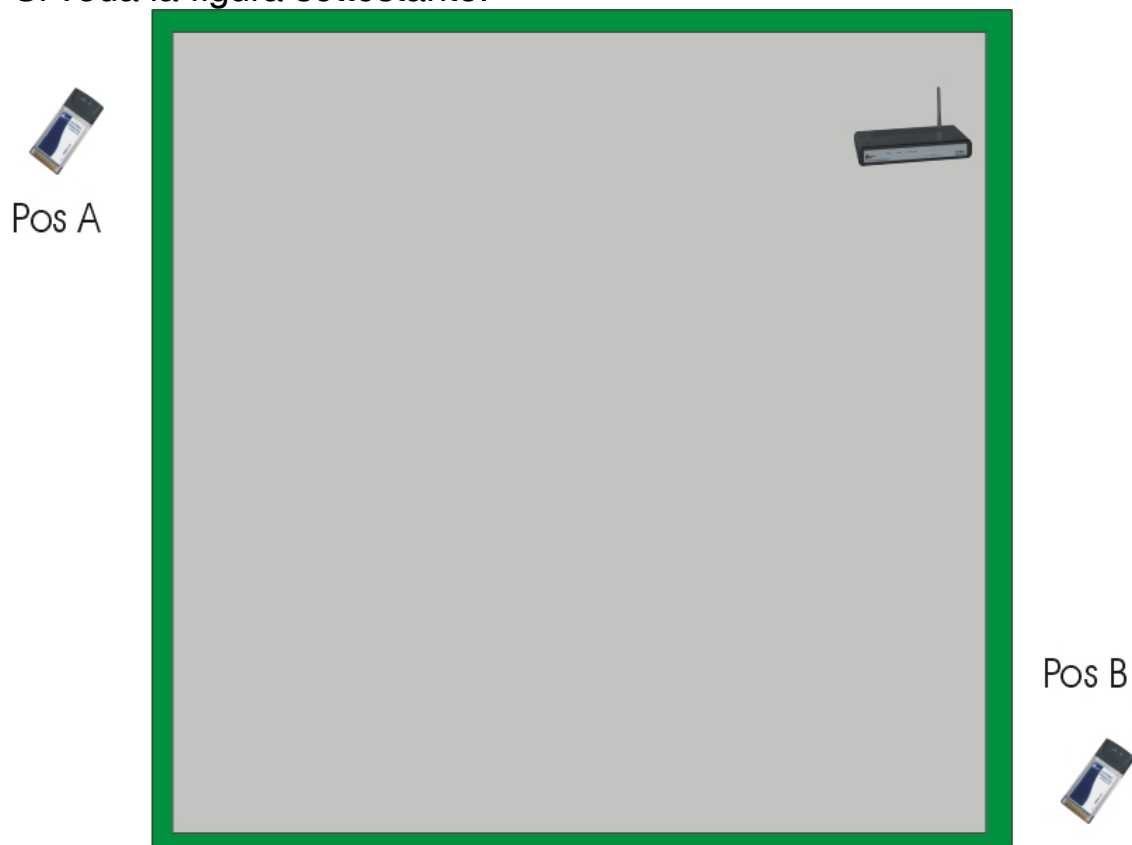
1.6 Considerazioni sull'Installazione

In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire un raggio di diverse decine di metri. E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine.

Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.

- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E' bene prendere in considerazione questo fatto.
- Allontanare il Wireless Broadband Router da ogni altro dispositivo che produca emissioni RF.
- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless Broadband Router col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante). Si veda la figura sottostante:



Il Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A. E' sufficiente collocare il Wireless Broadband Router al centro del locale per migliorare decisamente le prestazioni del client B.

CAPITOLO 2: Uso del Wireless Broadband Router

2.1 Precauzioni nell'uso del Wireless Broadband Router

- Non usare il Wireless Broadband Router in un luogo in cui ci siano condizioni di alte temperatura ed umidità, il Wireless Broadband Router potrebbe funzionare in maniera impropria e danneggiarsi.
- Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del Wireless Broadband Router.
- Non aprire mai il case del Wireless Broadband Router né cercare di ripararlo da soli.
- Se il Wireless Broadband Router dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.
- Non appoggiare il dispositivo su superfici plastiche o in legno che potrebbero non favorire lo smaltimento termico.
- Mettere il Wireless Broadband Router su una superficie piana e stabile oppure fissarlo a muro tramite le apposite scanalature sul pannello inferiore.
- Usare esclusivamente l'alimentatore fornito nella confezione, l'uso di altri alimentatori farà automaticamente decadere la garanzia.
- Non effettuare upgrade del firmware utilizzando apparati/client wireless ma solo wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.

2.2 I LED frontali

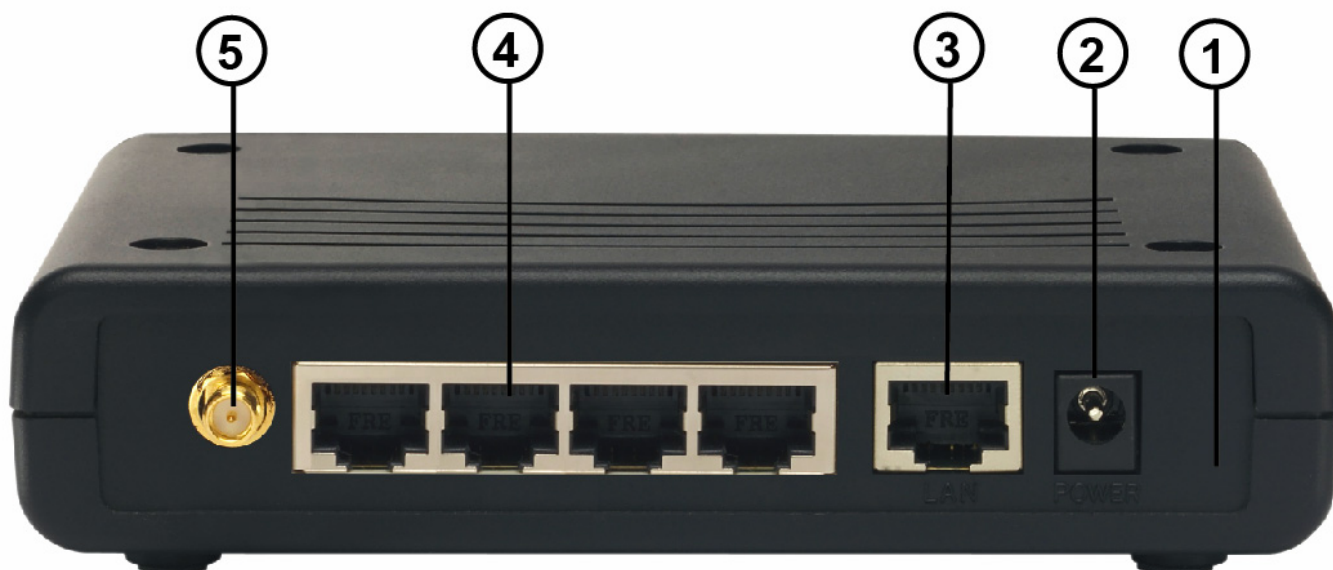
Sul pannello frontale del Wireless Broadband Router sono presenti tutta una serie di Led che indicano lo stato di alcune funzionalità del prodotto.

L'immagine e la tabella seguenti descrivono i LED posti sul pannello frontale del Wireless Broadband Router.



LED	INFORMAZIONE
POWER	Acceso quando connesso alla rete elettrica.
STATUS	Lampeggiante quando il dispositivo funziona correttamente. Acceso verde fisso o spento quando il dispositivo ha problemi.
WAN	Acceso quando connesso ad un dispositivo Ethernet Verde= connessione a 10 o 100Mbps Lampeggiante quando vi è trasmissione/ricezione.
WLAN	Acceso lampeggiante quando il modulo wireless è correttamente caricato e quando vi è trasmissione/ricezione. Spento se il modulo wireless è disattivato.
LAN (1-4)	Acceso quando connesso ad un dispositivo Ethernet Verde= connessione a 10 o 100Mbps Lampeggiante quando vi è trasmissione/ricezione.

2.3 Le porte posteriori

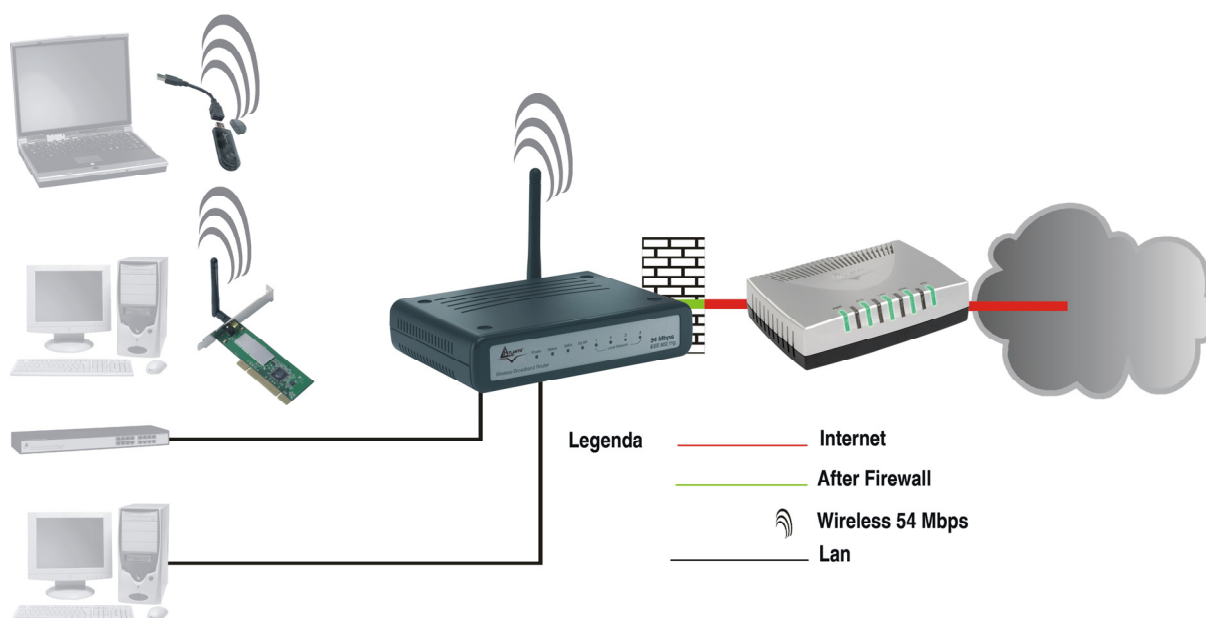


PORTE	UTILIZZO
POWER Jack(2)	Connettere l'alimentatore a questo jack.
WAN(3)	Connettere con un cavo UTP.
LAN(4)	Connettere con un cavo UTP.
Reverse SMA(5)	Collegare l'antenna fornita in dotazione.
Reset(1)	Dopo che il dispositivo è acceso, premere per effettuare il reset per una decina di secondi, rilasciare e questo punto il bottone. Tutti i LED si accenderanno e poi il sistema effettuerà un reboot caricando i parametri di default. Premere invece per un paio di secondi per effettuare il reboot dell'apparato.

2.4 Cablaggio

Anzitutto collegare alle porte RJ45 i PC della Lan oppure ulteriori Switch. Infine collegare l'alimentatore al Router ed alla presa elettrica. Una volta effettuati tutti i collegamenti, il prodotto effettuerà una diagnostica la cui durata è di circa una decina di secondi. Terminata questa fase, il Led POWER sarà acceso verde fisso ed il Led STATUS comincerà a lampeggiare indicando il corretto funzionamento del prodotto. I Led LAN/WLAN/WAN saranno accesi (a seconda dei collegamenti fatti) o lampeggianti.

In figura è possibile osservare una tipica installazione domestica, sulla cui porta WAN dell'apparato è stato collegato un dispositivo A02-RA141/A02-RA111 responsabile della connettività ADSL2+.



CAPITOLO 3: Configurazione

Il Wireless Broadband Router può essere configurato via browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet. Il prodotto offre una semplice interfaccia di configurazione.

3.1 Prima di iniziare

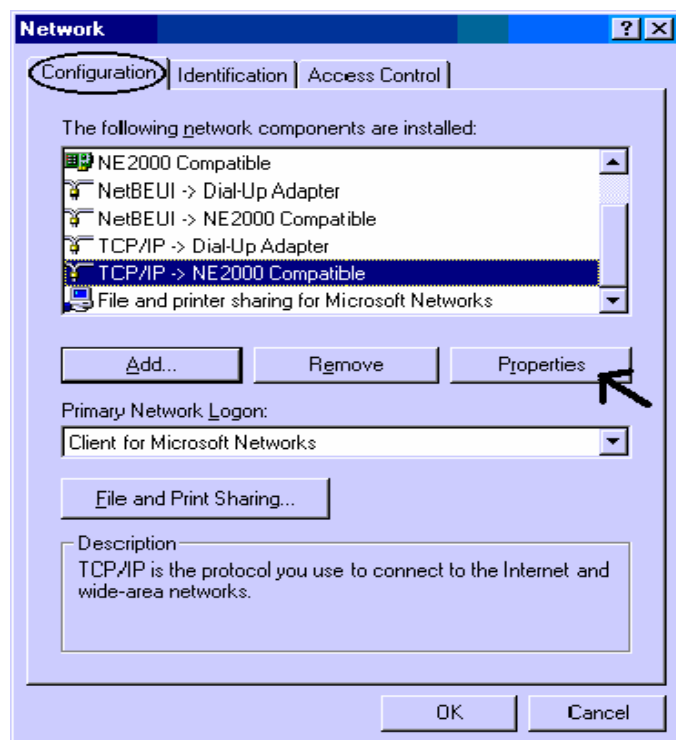
Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è connesso il Wireless Broadband Router. Tutti i PC devono avere una scheda di rete Ethernet installata correttamente, essere connessi al Wireless Broadband Router direttamente in wired/wireless o tramite un Hub/Switch ed avere il protocollo TCP/IP installato e correttamente configurato in modo da ottenere un indirizzo IP tramite il DHCP Server residente sul prodotto. Nel caso in cui il PC abbia già un indirizzo IP, questo deve stare nella stessa subnet del Wireless Broadband Router (il cui indirizzo IP di default è 192.168.1.1 e subnet mask 255.255.255.0). Certamente la strada più semplice per configurare i PC è quella settarli come client DHCP cui l'IP (ed altri parametri) è assegnato dal Wireless Broadband Router.

Anzitutto è necessario preparare i PC inserendovi (qualora non ci fosse già) la scheda di rete wired. E' necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:

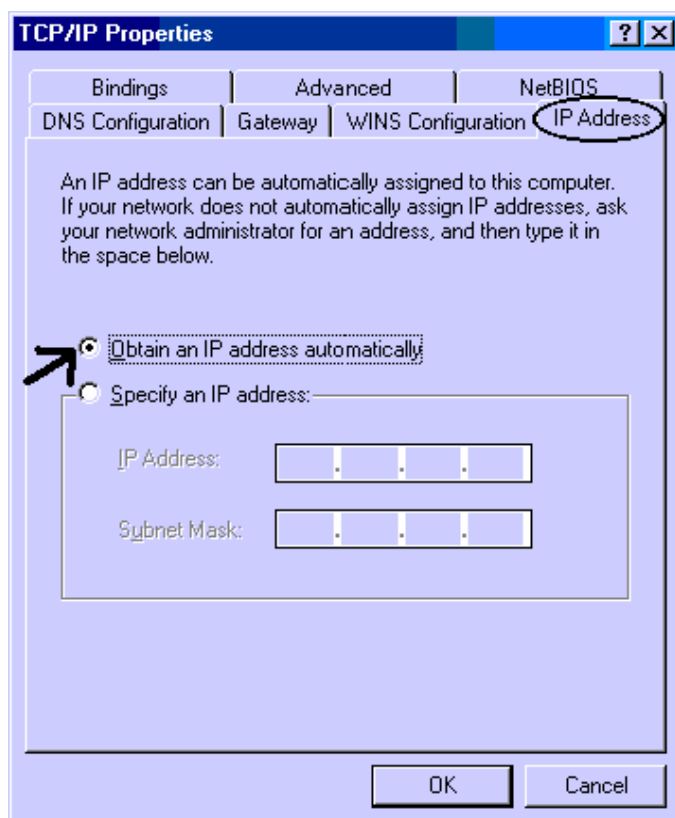


Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite il Wireless Broadband Router. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

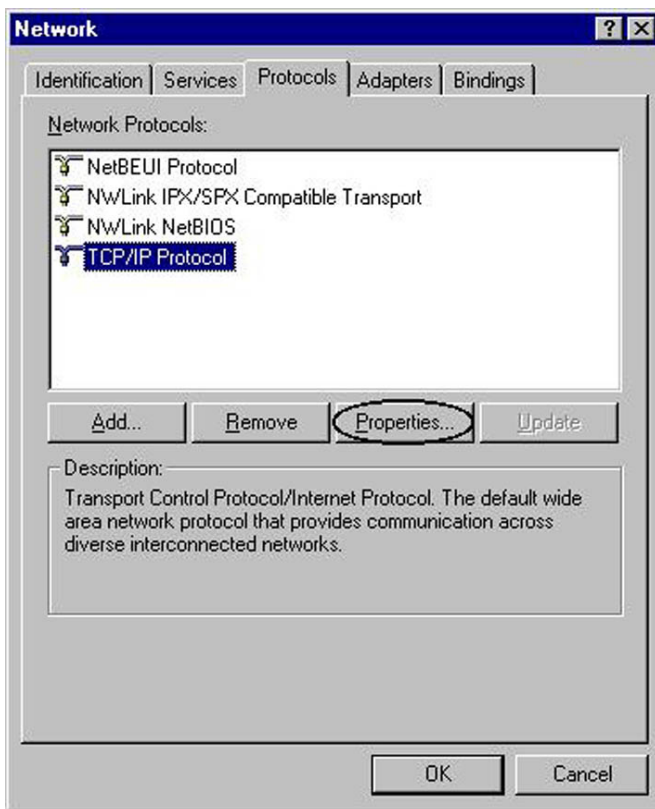
3.1.1 Configurazione del PC in Windows 95/98/ME



1. Andare in **Start/Settings/Control Panel**. Cliccare 2 volte su **Network** e scegliere **Configuration**.
2. Selezionare **TCP/IP** -> **NE2000 Compatible**, o qualsiasi Network Interface Card (NIC) del PC.
3. Cliccare su **Properties**.
4. Selezionare l'opzione **Obtain an IP address automatically** (dopo aver scelto IP Address).
5. Andare su **DNS Configuration**
6. Selezionare l'opzione **Disable DNS** e provvedere al riavvio della macchina al fine di apportare le modifiche effettuate.

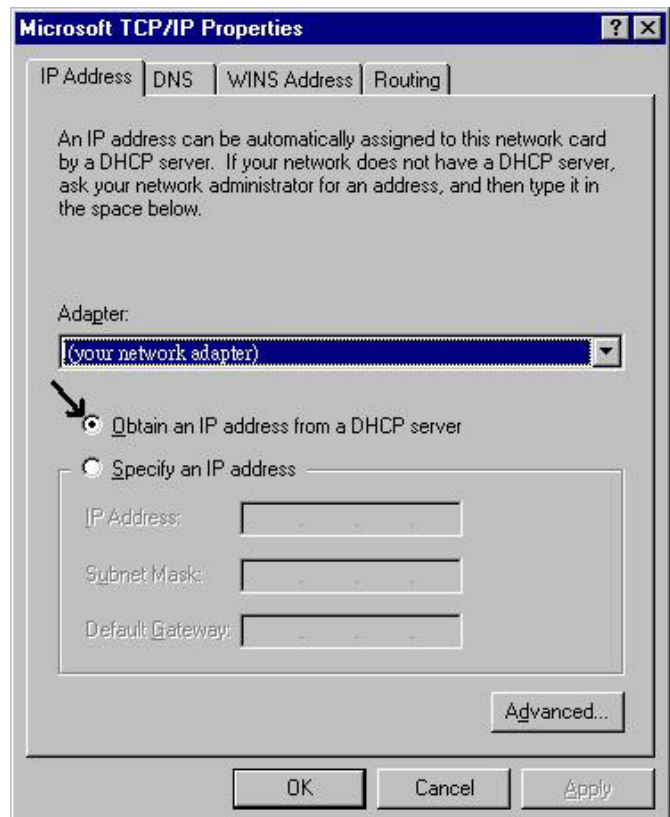


3.1.2 Configurazione del PC in Windows NT4.0



1. Andare su **Start/Settings/ Control Panel**. Cliccare per due volte su **Network** e poi cliccare su **Protocols**.
2. Selezionare **TCP/IP Protocol** e poi cliccare su **Properties**.

3. Selezionare l'opzione **Obtain an IP address from a DHCP server** e premere **OK**.

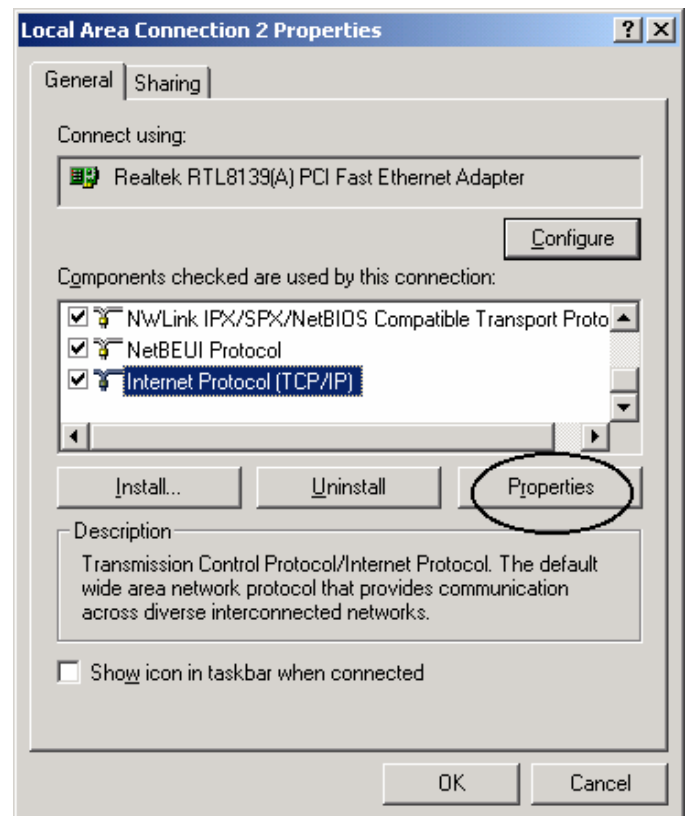
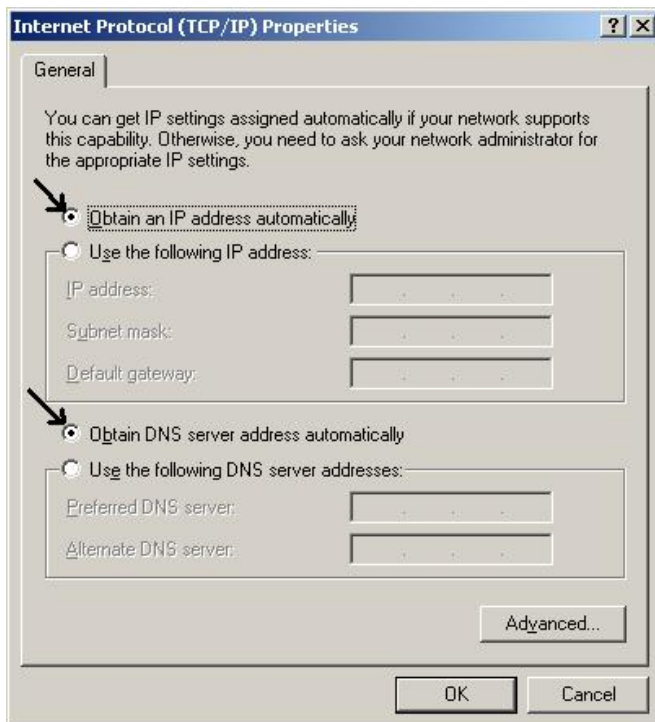


3.1.3 Configurazione del PC in Windows 2000



1. Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.
3. In **Local Area Connection Status** cliccare **Properties**.

4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**



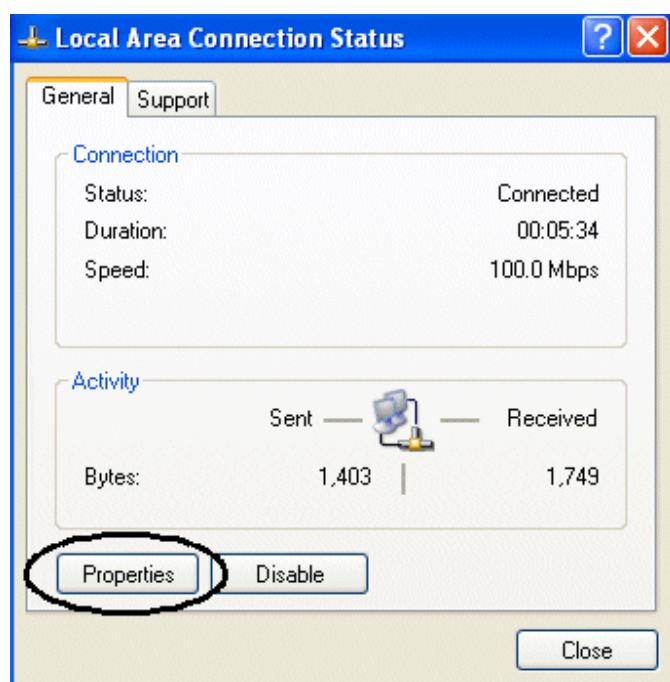
5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**

6. Premere su **OK** per terminare la configurazione

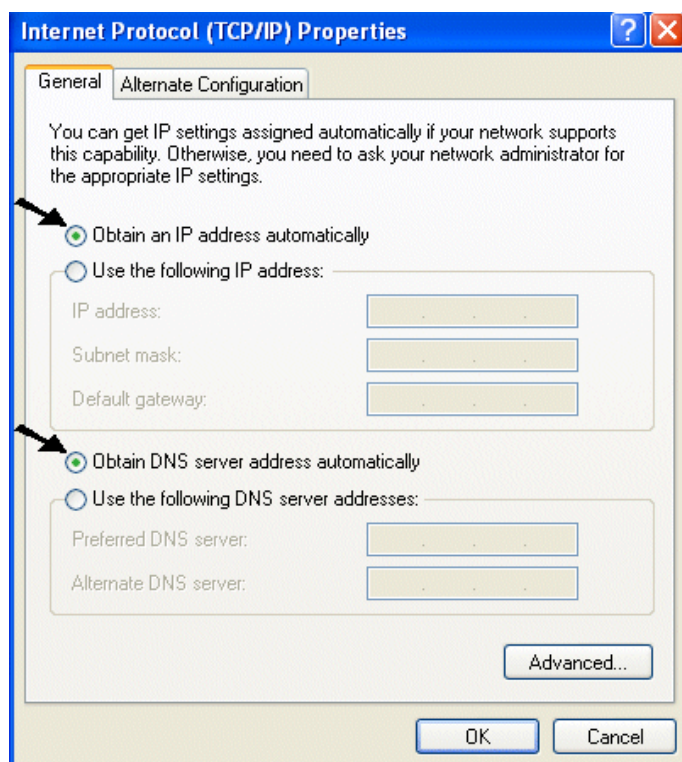
3.1.4 Configurazione del PC in Windows XP



1. Andare su **Start** e poi **Control Panel**. Cliccare due volte su **Network (in Classic View) Connections**.
2. Cliccare due volte su **Local Area Connection**.

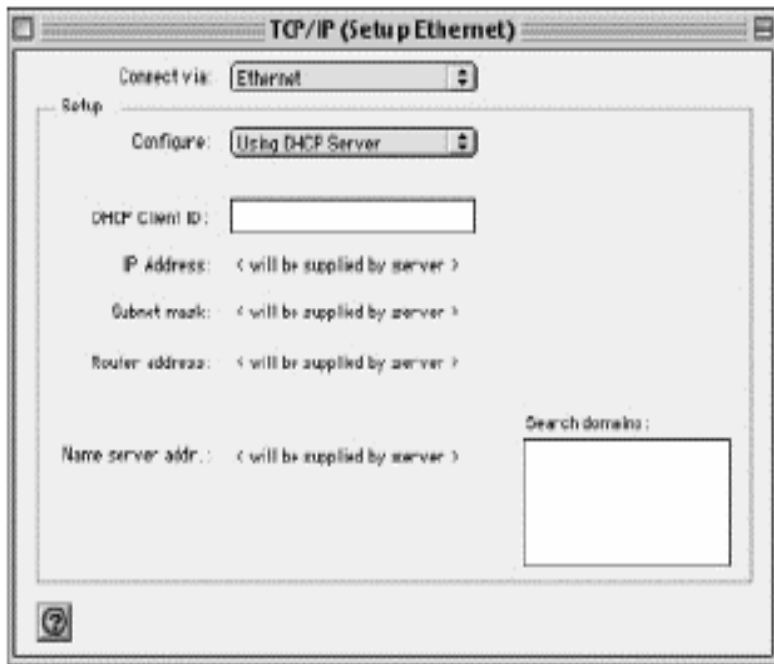


3. In **Local Area Connection Status** cliccare **Properties**.
4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.



5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**.
6. Premere su **OK** per terminare la configurazione

3.1.5 Configurazione in ambiente MAC



1. Cliccare sull'icona **Mela** nell'angolo in alto a sinistra dello schermo e selezionare: **Control Panel/TCP/IP**. Apparirà la finestra relativa al TCP/IP come mostrata in figura.
2. Scegliere **Ethernet** in **Connect Via**.
3. Scegliere **Using DHCP Server** in **Configure**.
4. Lasciare vuoto il campo **DHCP Client ID**.

3.1.6 Verifica della Configurazione

Per verificare il successo della configurazione (dopo aver riavviato il PC, operazione necessaria su Win98, 98Se, ME e invece sufficiente ottenere il rilascio dell'IP su XP, 2000), utilizzare il comando ping. Da una finestra Dos digitare:

ping 192.168.1.1

Se appare il seguente messaggio:

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
```

E' possibile procedere andando al punto seguente. Se invece appare il seguente messaggio:

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```


Controllare che il led LAN/WLAN sia acceso (cambiare il cavo qualora non fosse così). Controllare l'indirizzo del PC digitando **winipcfg** per (Win95,98,ME) o **ipconfig** (per Win2000,XP) ed eventualmente reinstallare lo stack TCP/IP.

3.2 Settaggi di Default

Prima di iniziare la configurazione del Wireless Broadband Router è necessario conoscere quali siano i settaggi di default:

- Nome Utente: **admin**
- Password: **admin**
- Indirizzo IP: **192.168.1.1**
- Subnet Mask: **255.255.255.0**
- Indirizzo IP WAN: **client DHCP**
- DHCP Server: **abilitato (192.168.1.100-192.168.1.199)**
- SSSID= **default**, Channel=6, WEP/WPA/WPA2=**disabilitato**

3.2.1 Password

Quando si configura il Wireless Broadband Router con il browser, introdurre username e password e premere su OK per entrare per la prima volta. E' consigliato cambiare la password, al fine di aumentare la sicurezza.



Qualora si perdesse la password premere per 10 (o più) secondi il bottone reset (utilizzando un cacciavite a punta e premendo delicatamente) per far tornare il Wireless Broadband Router alle impostazioni di default.

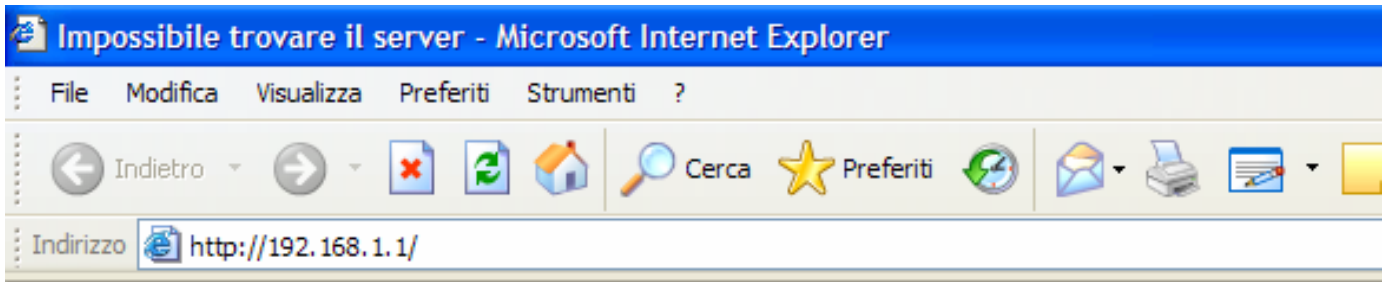
3.2.2 Porte LAN e WLAN

Questa tabella riassume i settaggi di default delle interfacce LAN e WLAN:

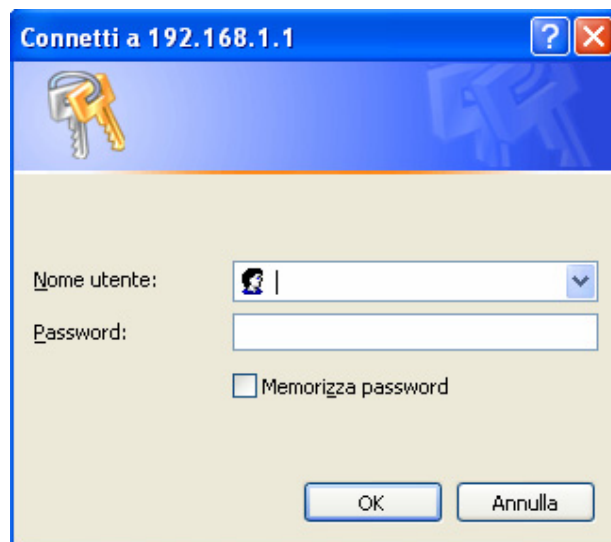
Porta LAN		Porta WLAN
IP address	192.168.1.1	Canale=6
Subnet Mask	255.255.255.0	SSID= default
		Sicurezza= Disabilitata

3.3 Configurazione tramite Browser

Accedere tramite Internet Explorer al seguente indirizzo IP (dove si inserisce l'URL) che di default è: “**192.168.1.1**”, e premere il tasto invio.



Introdurre il nome utente e la password (**admin, admin**) e premere **OK** per continuare.



Apparirà a questo punto l'interfaccia di configurazione dell'apparato. Chiudendo la Wizard è possibile accedere al Menù Principale dove è possibile configurare dettagliatamente il dispositivo (saltare la sezione immediatamente seguente). Nel caso il Wizard non fosse presente è sufficiente cliccare sull'apposita voce per avviarlo.

3.3.1 Setup Wizard

Grazie a questo Wizard è possibile configurare il dispositivo in brevissimo tempo. Appare l'immagine di sotto (qualora non fosse così, cliccare sul bottone Wizard).



Cliccare su **Next** per proseguire.

Step 1: Modifica Password

E' possibile adesso cambiare la password, cliccare poi su **Next** per passare al prossimo step.



Welcome to Setup Wizard

► Set Password

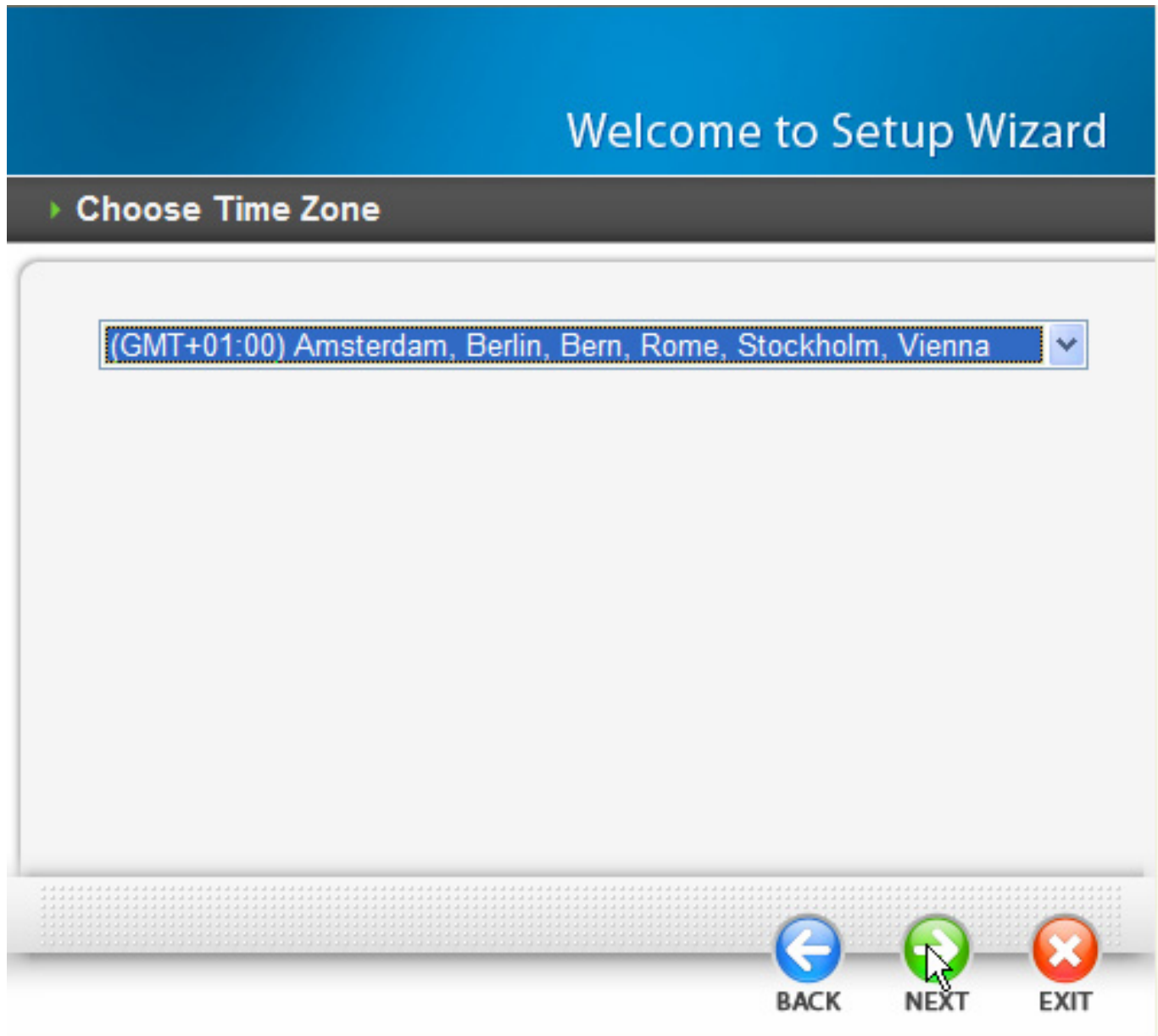
Password :

Verify Password :

BACK NEXT EXIT

Step2: Scelta della Time Zone


Selezionare adesso dal menù a tendina il fuso orario di appartenenza.



Cliccare su **Next** per proseguire.

Step 3: Configurazione LAN ed impostazioni del DHCP

E' possibile cambiare l'indirizzo IP del dispositivo e la subnet mask. Il valore di default è: **192.168.1.1**. Spuntare "**Enabled**" per abilitare il DHCP server del dispositivo. Il DHCP server assegnerà automaticamente gli indirizzi IP ai vari client Wireless o Wired. E' possibile assegnare il range di IP che saranno assegnati (inserite l'IP di partenza in "**Range start**" e l'IP finale in "**Range end**").



Welcome to Setup Wizard

► Set LAN & DHCP Server

LAN IP Address :

LAN Subnet Mask :

DHCP Server : Enabled Disabled

Range Start :

Range End :

BACK NEXT EXIT

Cliccare su **Next** per continuare.

Step 4: Impostazione della Connessione Internet

Il dispositivo avvierà in automatico un auto-detecting del tipo di connessione presente sulla porta WAN.



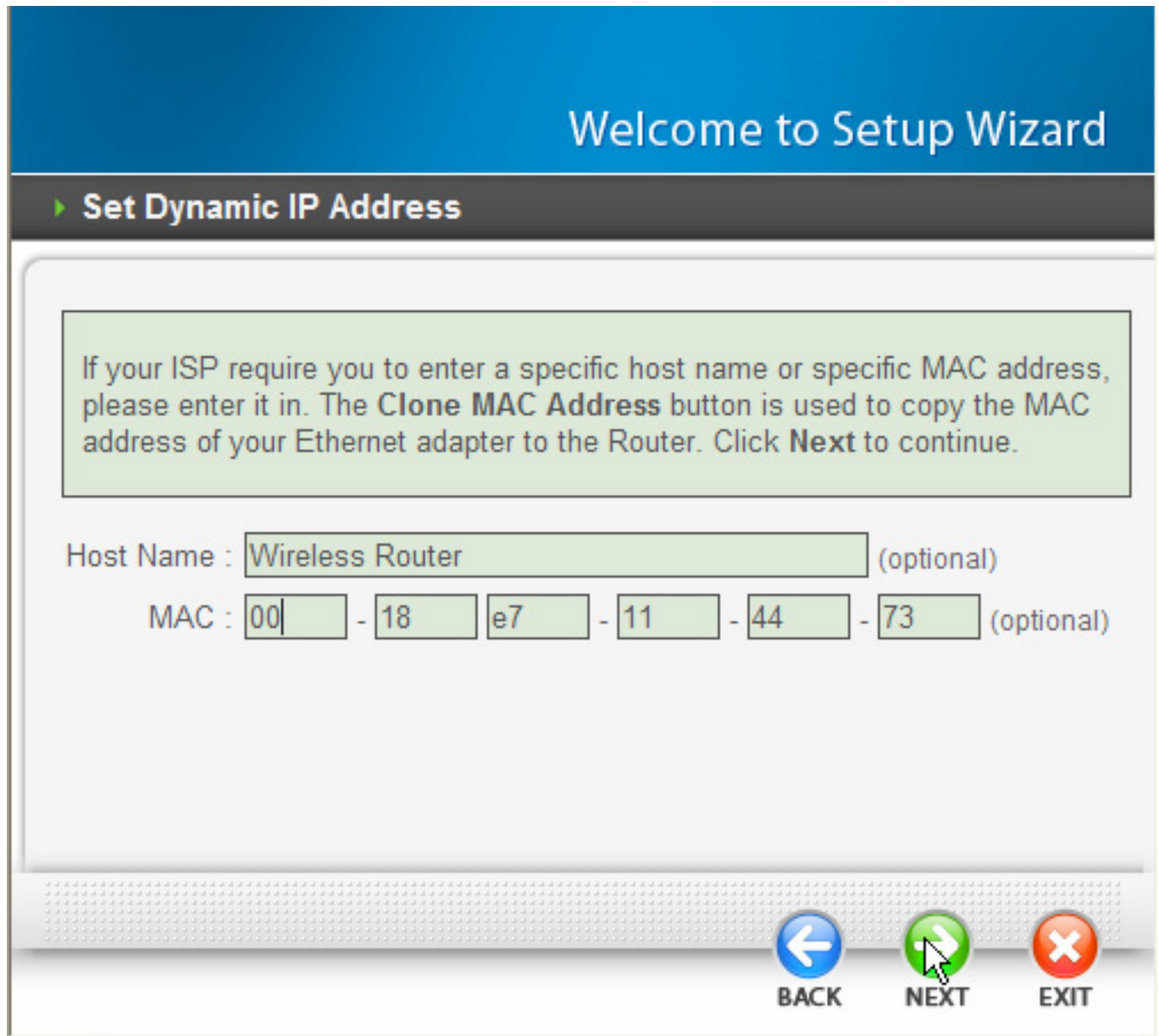
Dopo alcuni secondi, sarà possibile selezionare la modalità di connessione ad Internet tra le scelte disponibili. Se il dispositivo è utilizzato come Access Point (la porta WAN non viene collegata) saltare allo step (5) successivo.



Cliccare su **Next** per continuare.

Obtain IP automatically (DHCP client):

Scegliendo **Obtain IP automatically (DHCP client)**, l'interfaccia WAN prenderà l'indirizzo IP da un server DHCP presente sulla rete cui viene collegata.

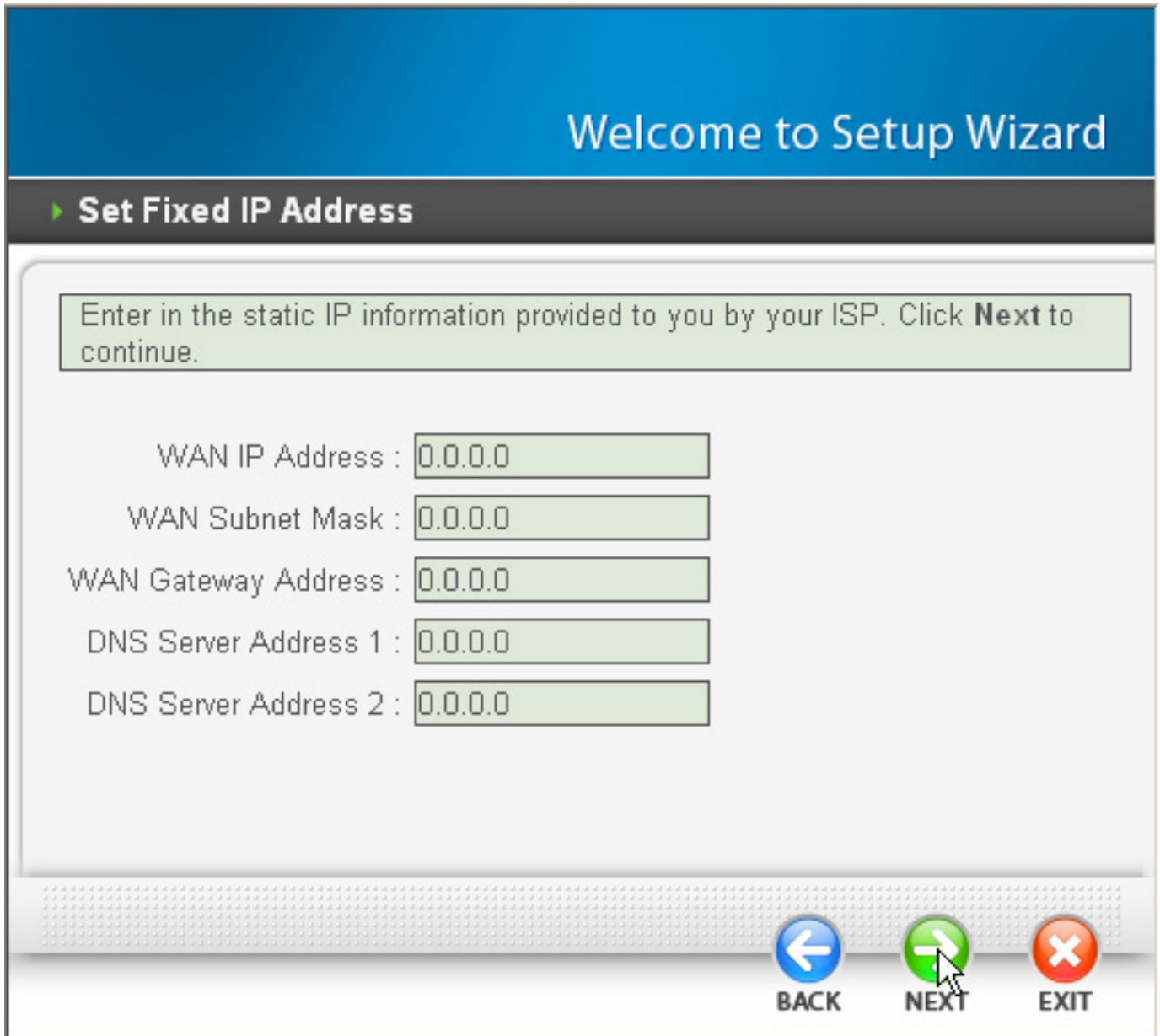


The screenshot shows a web-based setup wizard interface. At the top, a blue banner reads "Welcome to Setup Wizard". Below this, a dark grey bar contains the title "Set Dynamic IP Address" with a right-pointing arrow. The main content area has a light green background and contains a text box with instructions: "If your ISP require you to enter a specific host name or specific MAC address, please enter it in. The Clone MAC Address button is used to copy the MAC address of your Ethernet adapter to the Router. Click Next to continue." Below the text box, there are two input fields. The first is labeled "Host Name :" and contains the text "Wireless Router" followed by "(optional)". The second is labeled "MAC :" and contains the text "00" followed by a hyphen, "18" followed by a hyphen, "e7" followed by a hyphen, "11" followed by a hyphen, "44" followed by a hyphen, and "73" followed by "(optional)". At the bottom of the screen, there are three circular buttons: a blue "BACK" button with a left arrow, a green "NEXT" button with a right arrow and a mouse cursor, and a red "EXIT" button with a white 'X'.

A questo punto, è possibile clonare sul Wireless Broadband Router un indirizzo MAC particolare. Nel caso non ci fosse questa necessità proseguire cliccando **Next**.

Fixed IP:

Introdurre l'indirizzo IP, Subnet Mask e Gateway manualmente sull'interfaccia WAN. Introdurre anche gli IP dei DNS.



The screenshot shows a web-based setup wizard interface. At the top, a blue banner reads "Welcome to Setup Wizard". Below this, a dark grey bar contains the title "Set Fixed IP Address". A light green box contains the instruction: "Enter in the static IP information provided to you by your ISP. Click **Next** to continue." Below the instruction are five input fields, each with a label and a text box containing "0.0.0.0":
WAN IP Address : 0.0.0.0
WAN Subnet Mask : 0.0.0.0
WAN Gateway Address : 0.0.0.0
DNS Server Address 1 : 0.0.0.0
DNS Server Address 2 : 0.0.0.0
At the bottom right, there are three circular buttons: a blue "BACK" button with a left arrow, a green "NEXT" button with a right arrow and a mouse cursor over it, and a red "EXIT" button with a white 'X'.

Cliccare su **Next** per continuare.



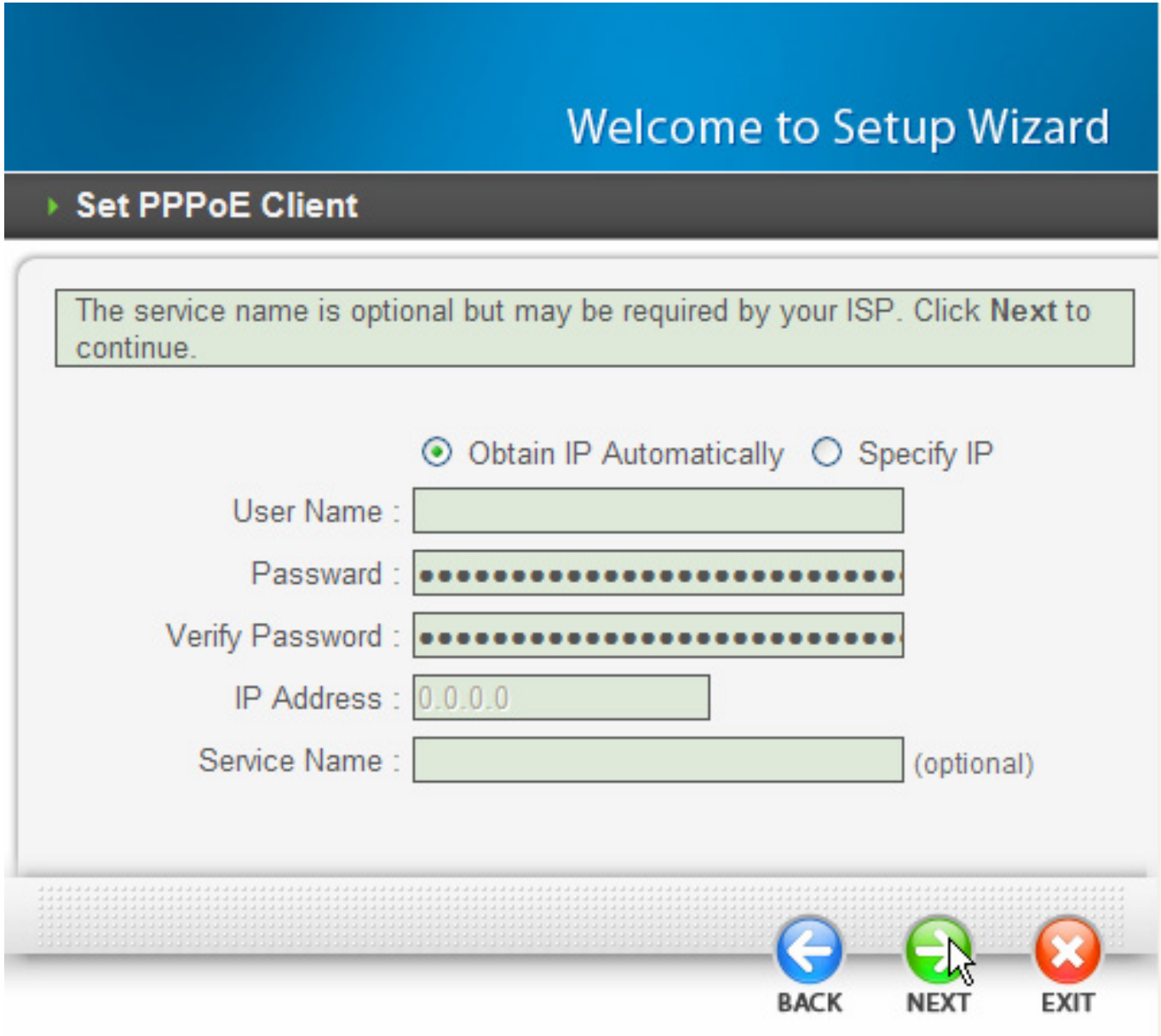
E' necessario inserire il server DNS primario (DNS Server Address 1).

PPPoE:

Introdurre l'Username e Password (ed il Service Name se espressamente richiesto dal fornitore del servizio) dell'abbonamento con l'ISP.

Sarà necessario reintrodurre la password per la verifica.

Nel caso fosse necessario un indirizzo IP statico, spuntare la voce **Specify IP** ed immettere nel campo IP Address il valore dello stesso.



Welcome to Setup Wizard

► Set PPPoE Client

The service name is optional but may be required by your ISP. Click Next to continue.

Obtain IP Automatically Specify IP

User Name :

Password :

Verify Password :

IP Address :

Service Name : (optional)

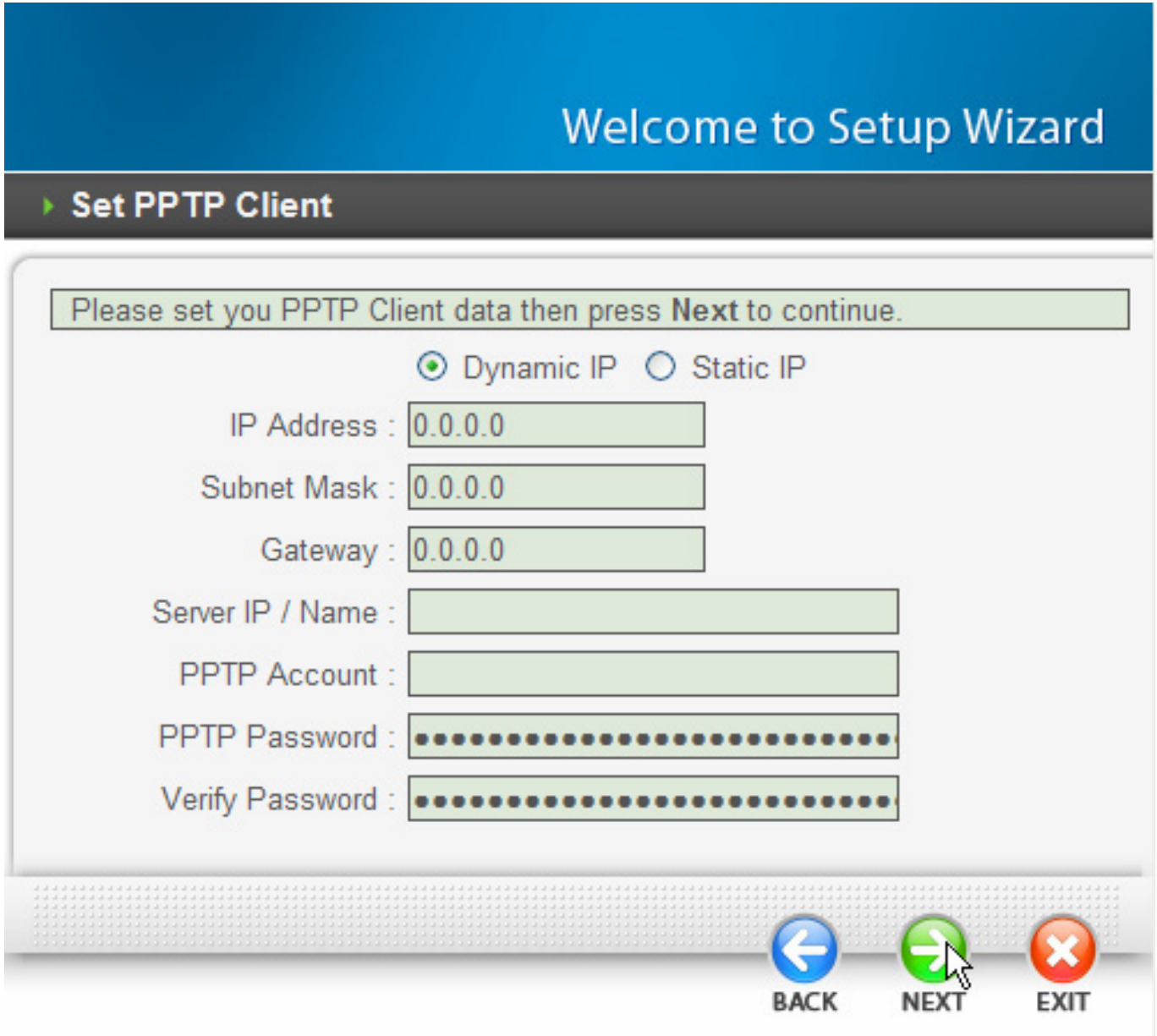
BACK NEXT EXIT

Cliccare su **Next** per continuare.

PPTP/L2TP:

Introdurre l'Username (PPTP Account) e Password ed il nome o IP (eventualmente l'IP) del server PPTP.

Spuntare la voce **Static IP** nel caso in sia richiesto un indirizzo IP statico dal server PPTP/L2TP.



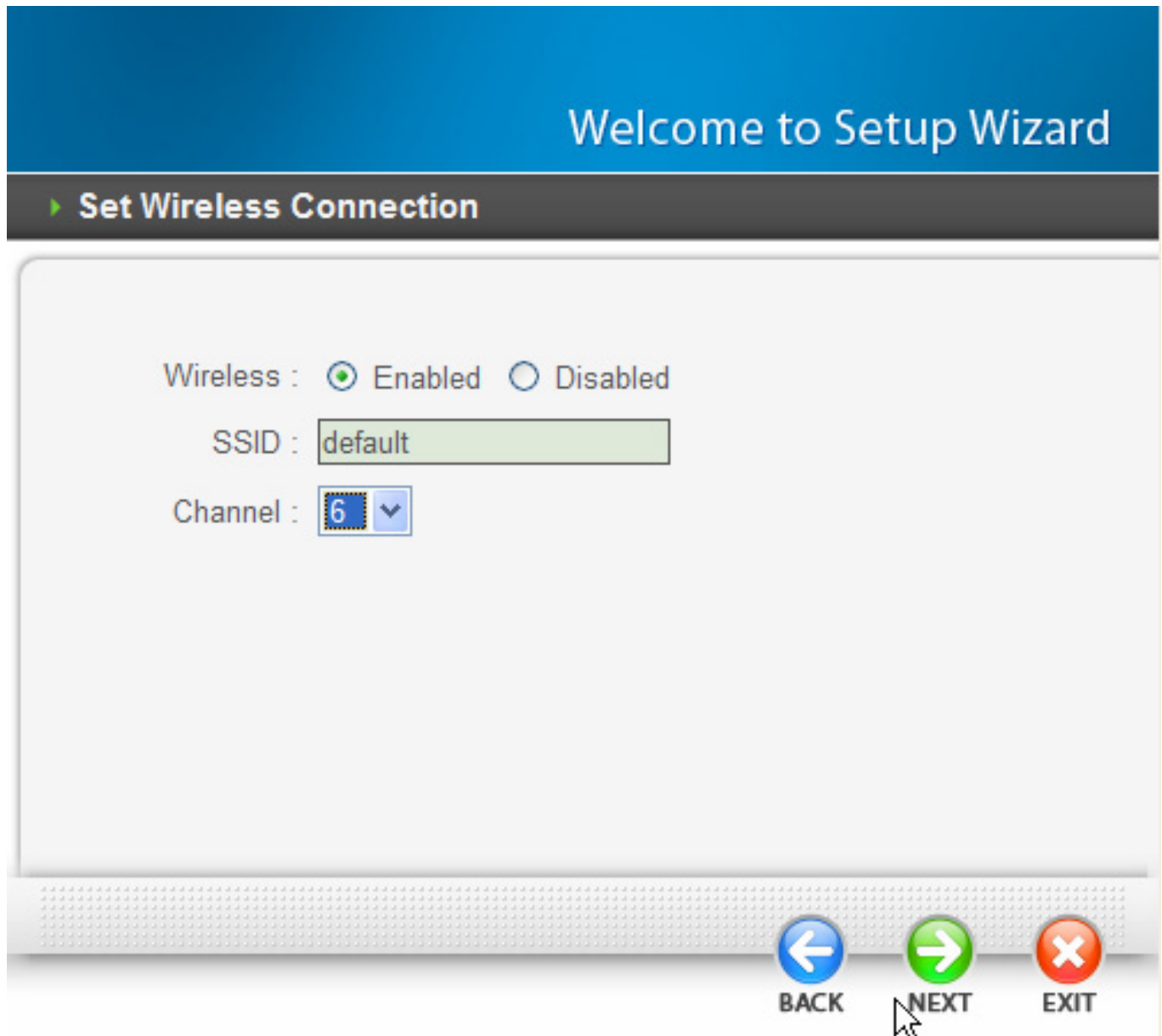
Cliccare su **Next** per continuare.



E' necessario inserire l'indirizzo del PPTP/L2TP Server.

Step 5: Set Wireless LAN connection

Cliccare **Enabled** per abilitare l'interfaccia wireless. Introdurre il valore di SSID (deve essere identico in tutti i dispositivi) e scegliere il canale su cui opererà il dispositivo.



Welcome to Setup Wizard

► Set Wireless Connection

Wireless : Enabled Disabled

SSID :

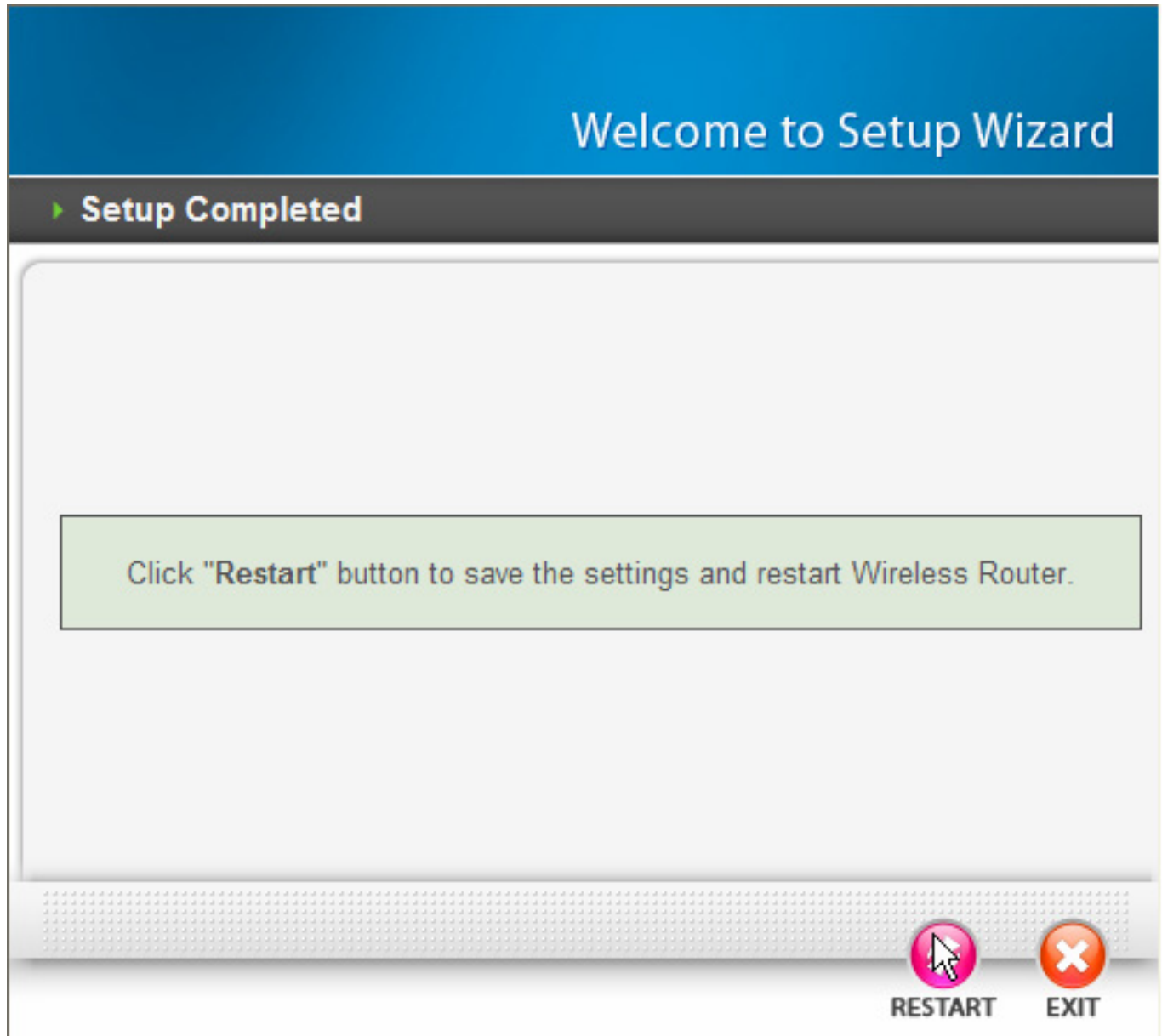
Channel : ▼

BACK NEXT EXIT

Cliccare su **Next** per continuare.

Step 6: Restart

A questo punto la configurazione è terminata; riavviare il Wireless Broadband Router premendo su **Restart**. Cliccando invece su **Exit** tutti i settaggi impostati non verranno salvati.



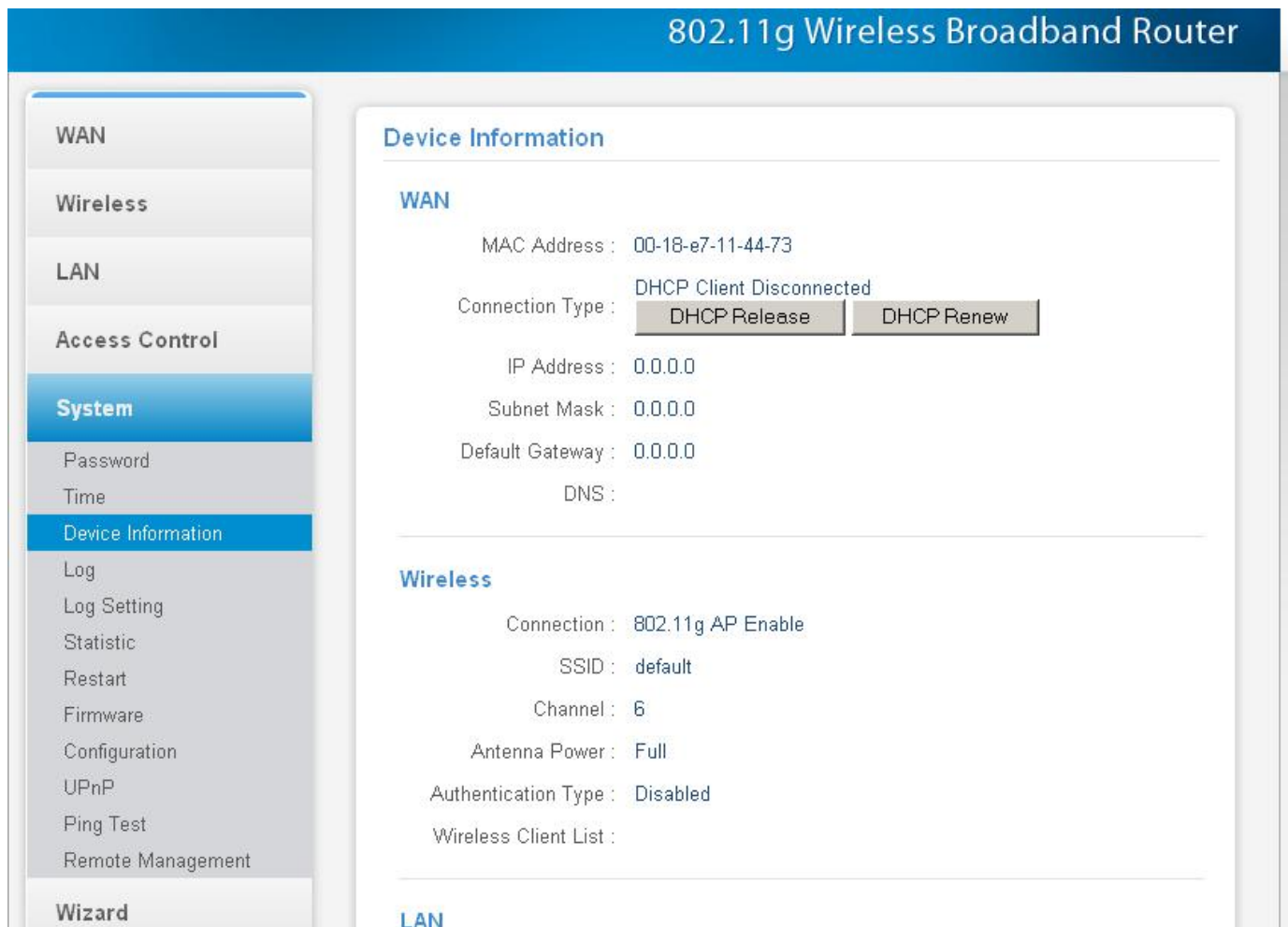
Provare ad effettuare una prova di navigazione.

3.3.2 Navigare nell'interfaccia Web di Configurazione

Questa sezione descrive come navigare all'interno dell'interfaccia di configurazione.

Sono disponibili 6 differenti menu:

- **WAN**
- **Wireless**
- **LAN**
- **Access Control**
- **System**
- **Wizard**



Cliccando sulla sezione desiderata, nello spazio della homepage saranno visualizzati i settaggi relativi alla configurazione della sezione scelta. Una volta effettuata la configurazione della sezione opportuna, cliccare su **Apply** per salvare i settaggi.

3.4 WAN

3.4.1 Connection Type

In questa sezione è possibile configurare la sezione WAN dell'apparato.

Connection Type

Connection Type :

WAN IP Address : Obtain IP Automatically Specify IP

IP Address :

Subnet Mask :

Gateway :

DNS 1 :

DNS 2 :

Clone MAC Address :

<input type="text" value="00"/>	-	<input type="text" value="18"/>	-	<input type="text" value="e7"/>	-	<input type="text" value="11"/>	-	<input type="text" value="44"/>	-	<input type="text" value="73"/>	<input type="button" value="Clone MAC Address"/>
---------------------------------	---	---------------------------------	---	---------------------------------	---	---------------------------------	---	---------------------------------	---	---------------------------------	--



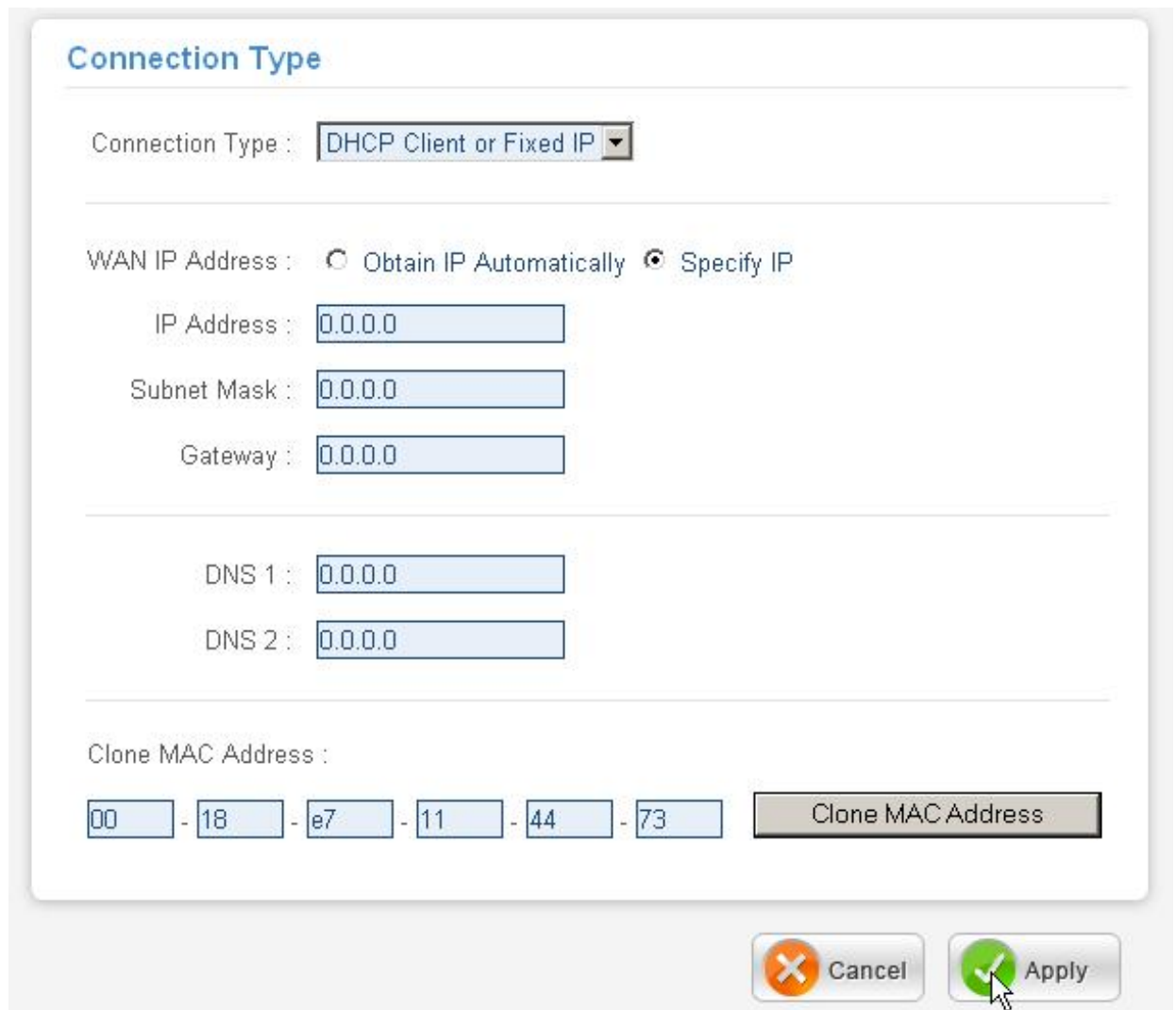
Connection Type:

E' possibile scegliere tra le seguenti opzioni **DHCP client or Fixed IP, PPPoE, PPTP, L2TP e BigPond Cable** presenti nel menù a tendina:

- **DHCP client or Fixed IP**

Scegliendo questa modalità è necessario inserire (dopo aver spuntato la voce **Specify IP**) gli indirizzi IP della parte WAN e gli indirizzi dei server DNS. Scegliendo invece **Obtain IP automatically**, il router riceverà sull'interfaccia WAN l'IP da un opportuno server DHCP.

Se necessario, è possibile clonare un particolare indirizzo MAC inserendolo nel campo apposito e premendo il tasto **Clone MAC Address**.



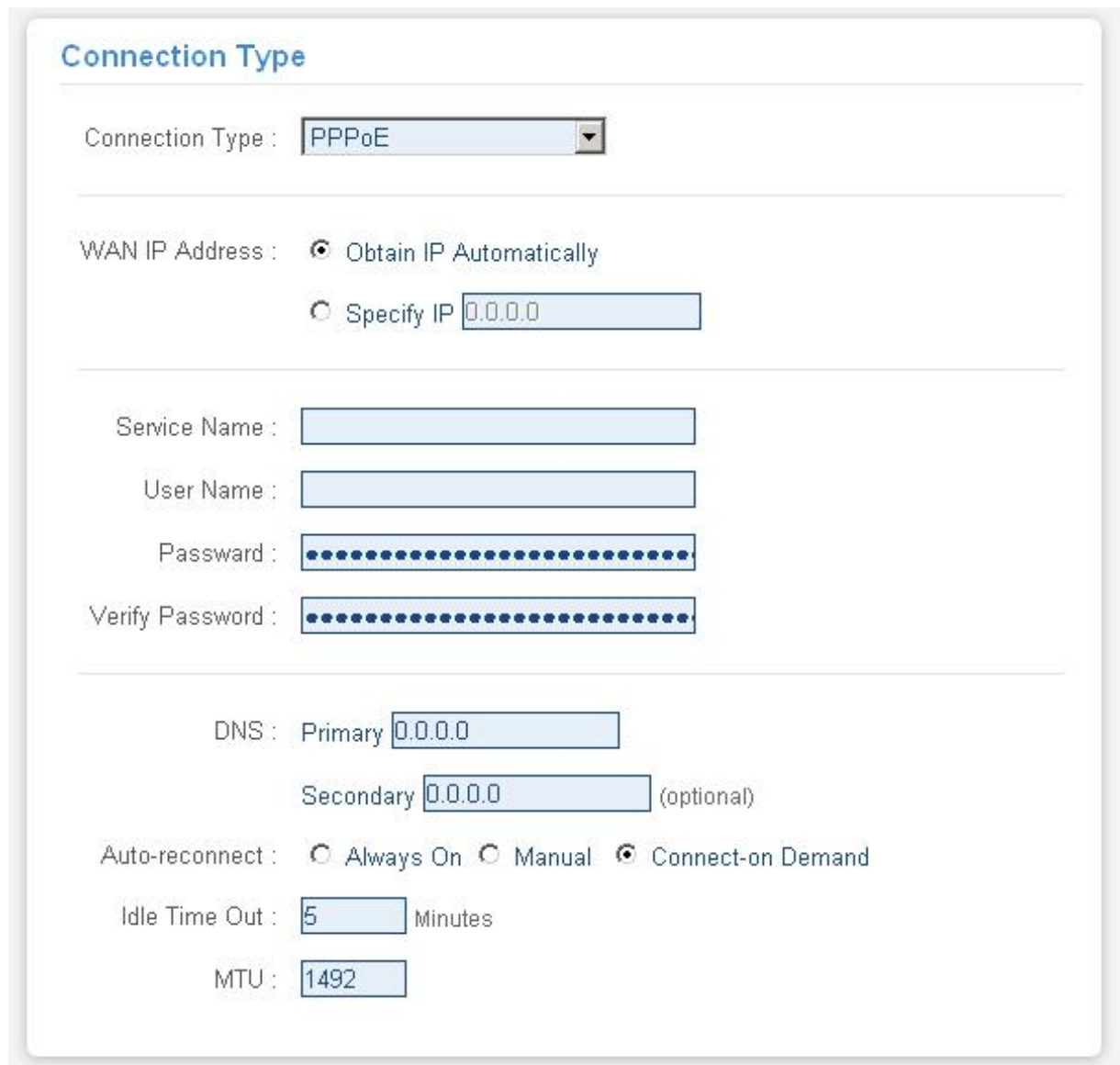
Cliccare su **Apply** per salvare le modifiche.



In caso si selezioni la voce **Specify IP**, è necessario inserire il server DNS primario (DNS Server Address 1).

- **PPPoE**

E' necessario collegare l'apparato ad un modem Ethernet (settato come Bridge) ed introdurre tutti i parametri relativi al collegamento ADSL PPPoE con l'ISP. In questo modo l'indirizzo IP che l'ISP assegnerà (dinamico o statico) sarà preso dall'interfaccia WAN del Wireless Broadband Router.



The screenshot shows the 'Connection Type' configuration page. The 'Connection Type' dropdown is set to 'PPPoE'. Under 'WAN IP Address', the 'Obtain IP Automatically' radio button is selected, and the 'Specify IP' field contains '0.0.0.0'. There are four empty input fields for 'Service Name', 'User Name', 'Password', and 'Verify Password'. The 'DNS' section has 'Primary' set to '0.0.0.0' and 'Secondary' set to '0.0.0.0' (optional). The 'Auto-reconnect' section has 'Connect-on Demand' selected. 'Idle Time Out' is set to '5' minutes and 'MTU' is set to '1492'.

Wan IP Address: Spuntare la voce **Obtain IP automatically** nel caso in cui l'indirizzo IP venga assegnato dinamicamente dall'ISP. Scegliere invece la voce **Specify IP** per inserire manualmente l'indirizzo IP statico.

Service Name: Immettere il valore del campo solo se specificatamente richiesto dall'ISP.

User Name: Inserire il nome utente fornito dall'ISP.

Password: Inserire la password fornita dall'ISP.

Verify Password: Reinserire la password immessa nel campo **Password**

DNS: Inserire gli indirizzi dei server DNS (vengono richiesti un DNS primario e uno opzionale secondario).

Auto-reconnect: Selezionare la modalità di connessione del prodotto alla rete Internet. E' possibile scegliere tra: **Always On**, **Manual** o **Connect-on Demand**.

Idle Time Out: Immettere un valore (espresso in minuti), al termine del quale, nel caso di mancato passaggio di pacchetti, il Router interromperà la connessione PPPoE (Questa opzione non è verrà utilizzata nella modalità **Always On**).

MTU: Inserire il valore della Maximum Transfert Unit (è consigliabile non modificare il valore proposto).

Cliccare su **Apply** per salvare le modifiche.

Per ulteriori dettagli consultare l'Appendice D. Richiedere tutti i parametri necessari al proprio ISP (Username, password).



Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

- **PPTP/L2TP**

E' necessariamente collegare l'apparato ad un opportuno modem/Router Ethernet . Per dettagli consultare il manuale dell'apparato e richiedere tutti i dettagli al proprio ISP (Username, password).

Connection Type

Connection Type :

WAN IP Address : Obtain IP Automatically Specify IP

IP Address :

Subnet Mask :

Gateway :

DNS :

Server IP/Name :

PPTP Account :

PPTP Password :

Verify Password :

Auto-reconnect : Always On Manual Connect-on Demand

Idle Time Out : Minutes

MTU :

Wan IP Address: Spuntare la voce **Obtain IP automatically** nel caso in cui l'indirizzo IP venga assegnato dinamicamente. Scegliere invece la voce **Specify IP** per inserire manualmente l'indirizzo IP statico.

Server IP/Name: Inserire il nome di dominio o l'indirizzo IP del server PPTP/L2TP.

PPTP/L2TP Account: Inserire la UserName per l'autenticazione PPTP/L2TP.

PPTP/L2TP Password: Inserire la password per l'autenticazione PPTP/L2TP.

Verify Password: Confermare la password immessa nel campo precedente.

Auto-reconnect: Selezionare la modalità di connessione del prodotto alla rete Internet. E' possibile scegliere tra: **Always On**, **Manual** o **Connect-on Demand**.

Idle Time Out: Immettere un valore (espresso in minuti), al termine del quale, nel caso di mancato passaggio di pacchetti, il Router interromperà la connessione PPTP/L2TP (Questa opzione non verrà utilizzata nella modalità **Always On**).

MTU: Inserire il valore della Maximum Transfert Unit (è consigliabile non modificare il valore proposto).

Cliccare su **Apply** per salvare le modifiche.



Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiasi problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.



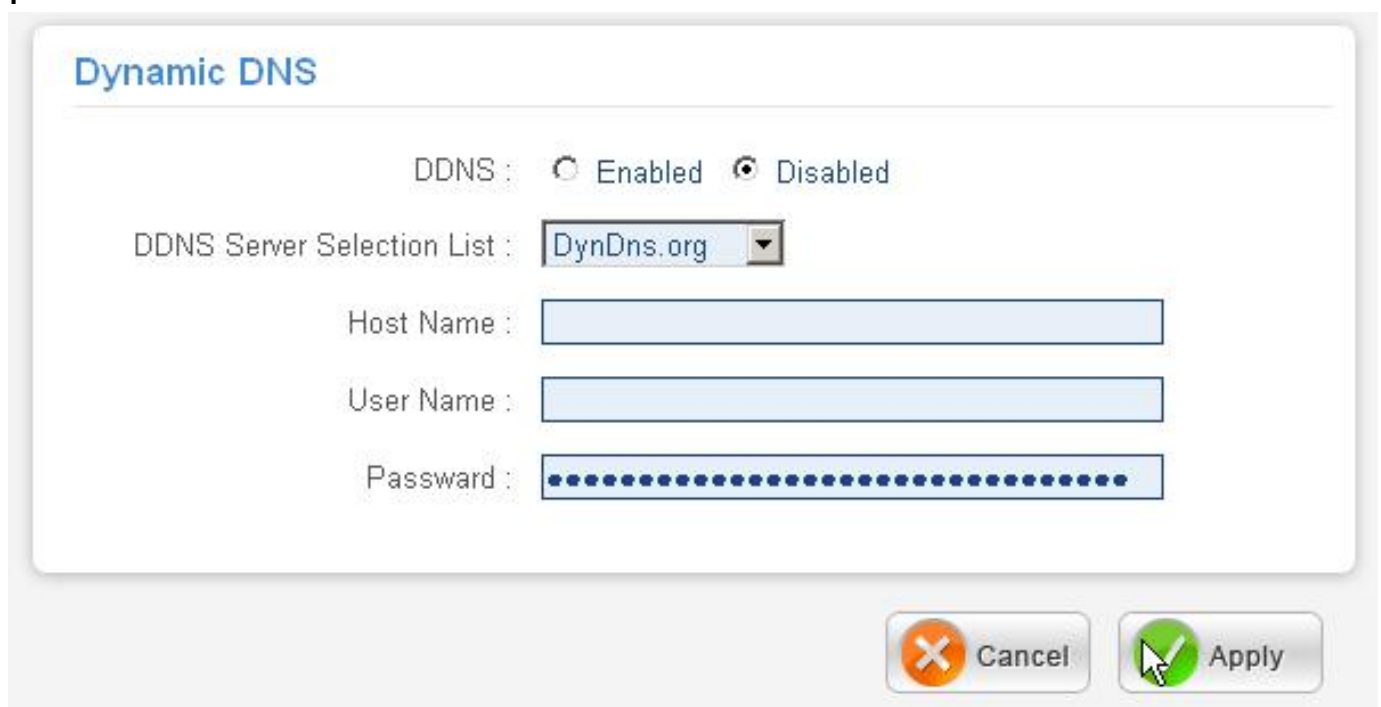
E' necessario inserire l'indirizzo del PPTP/L2TP Server.

3.4.2 Dynamic DNS

In questa sezione è possibile configurare un account Dynamic DNS.



Per il corretto utilizzo di questa funzionalità, è necessario registrare preventivamente un dominio DDNS. Fare riferimento all'**APPENDICE H** per un esempio di registrazione.



DDNS: Cliccare **Enabled** per abilitare il client Dynamic DNS.

DDNS Server Selection List: Selezionare dalla lista il Server DDNS da utilizzare.

Host Name: Inserire l'host Dynamic DNS da utilizzare (è necessario che il dominio sia stato preventivamente registrato sul sito del fornitore di servizio).

User Name: Inserire la UserName necessaria per l'autenticazione dell'account Dynamic DNS.

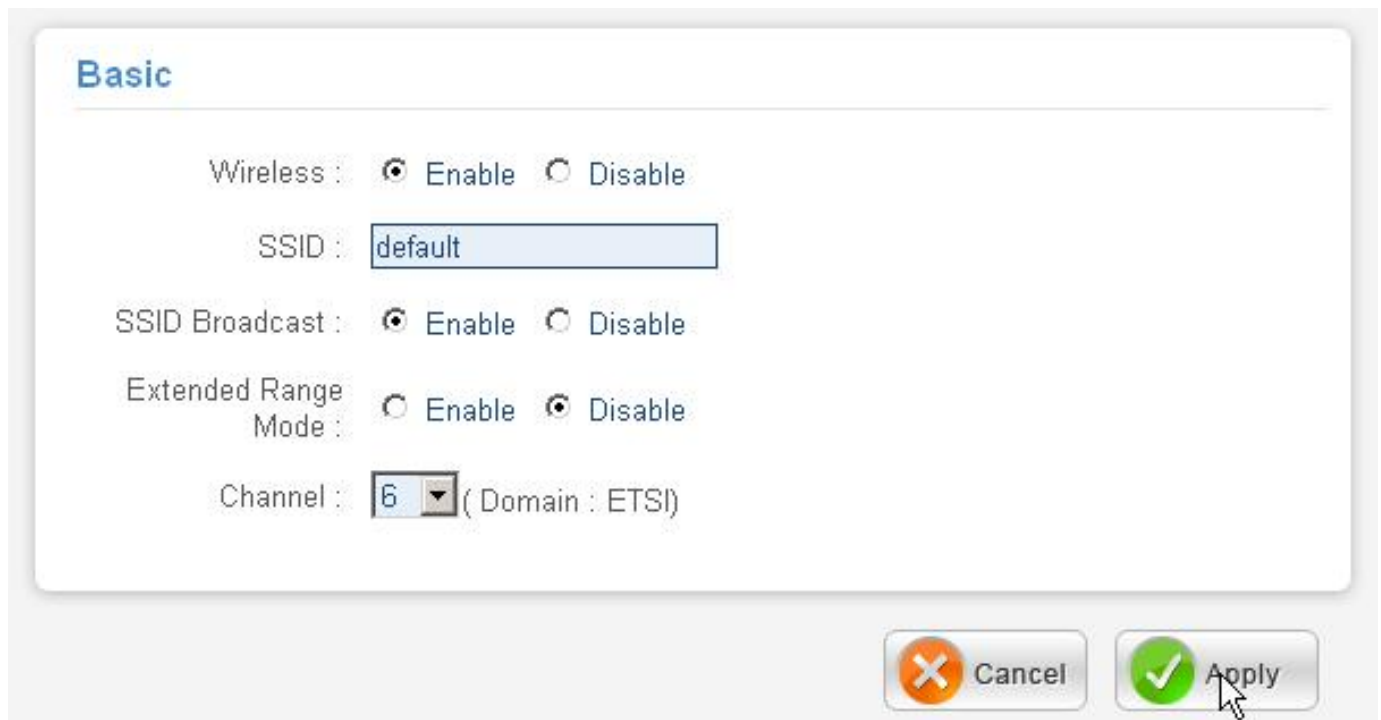
Password: Inserire la password necessaria per l'autenticazione dell'account Dynamic DNS.

Cliccare su **Apply** per salvare le modifiche.

3.5 Wireless

3.5.1 Basic

In questa sezione è possibile configurare l'interfaccia wireless dell'apparato.



The screenshot shows a web interface for configuring wireless settings. The title is "Basic". The settings are as follows:

- Wireless : Enable Disable
- SSID :
- SSID Broadcast : Enable Disable
- Extended Range Mode : Enable Disable
- Channel : (Domain : ETSI)

At the bottom right, there are two buttons: "Cancel" (with a red X icon) and "Apply" (with a green checkmark icon). A mouse cursor is pointing at the "Apply" button.

Wireless: Cliccare **Enable** per abilitare l'interfaccia wireless.

SSID: Introdurre il valore di SSID. Ogni dispositivo che vorrà accedere al router dovrà contenere questo valore nel proprio campo SSID.

SSID Broadcast: Cliccare **Enable** per abilitare l'SSID Broadcast. Nel caso si necessiti che l'SSID della rete non venga rilevato durante uno scanning delle reti disponibili, selezionare **Disable**.

Extended Range Mode: Cliccare **Enable** per abilitare la modalità Atheros XR® (eXtended Range). Questa modalità è utilizzabile solo con client Atheros e permette di ottenere una diminuzione delle zone morte e un incremento del raggio di copertura del prodotto.

Channel: Selezionare il canale per la trasmissione wireless.

Cliccare su **Apply** per salvare le modifiche.



Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11g/b è suddiviso in “canali”. Il numero di canali disponibili dipende dall’ area geografica di appartenenza. E’ possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point/ Wireless Broadband Router vicini. L’interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata “Overlap”.

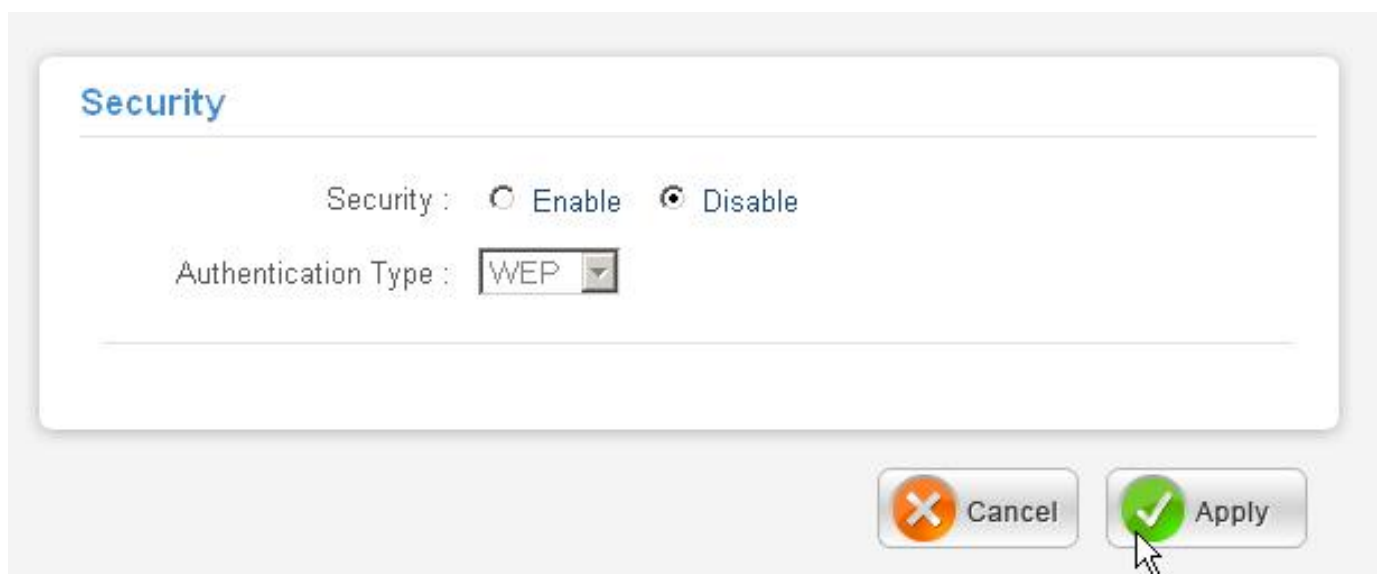
E’ consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6).

Da questo si evince che soltanto 3 Access Point/Wireless Router possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali (funzionamento contemporaneo).

3.5.2 Security

Il prodotto supporta i più recenti standard di sicurezza per quanto riguarda le trasmissioni wireless (WEP, WPA e WPA2).

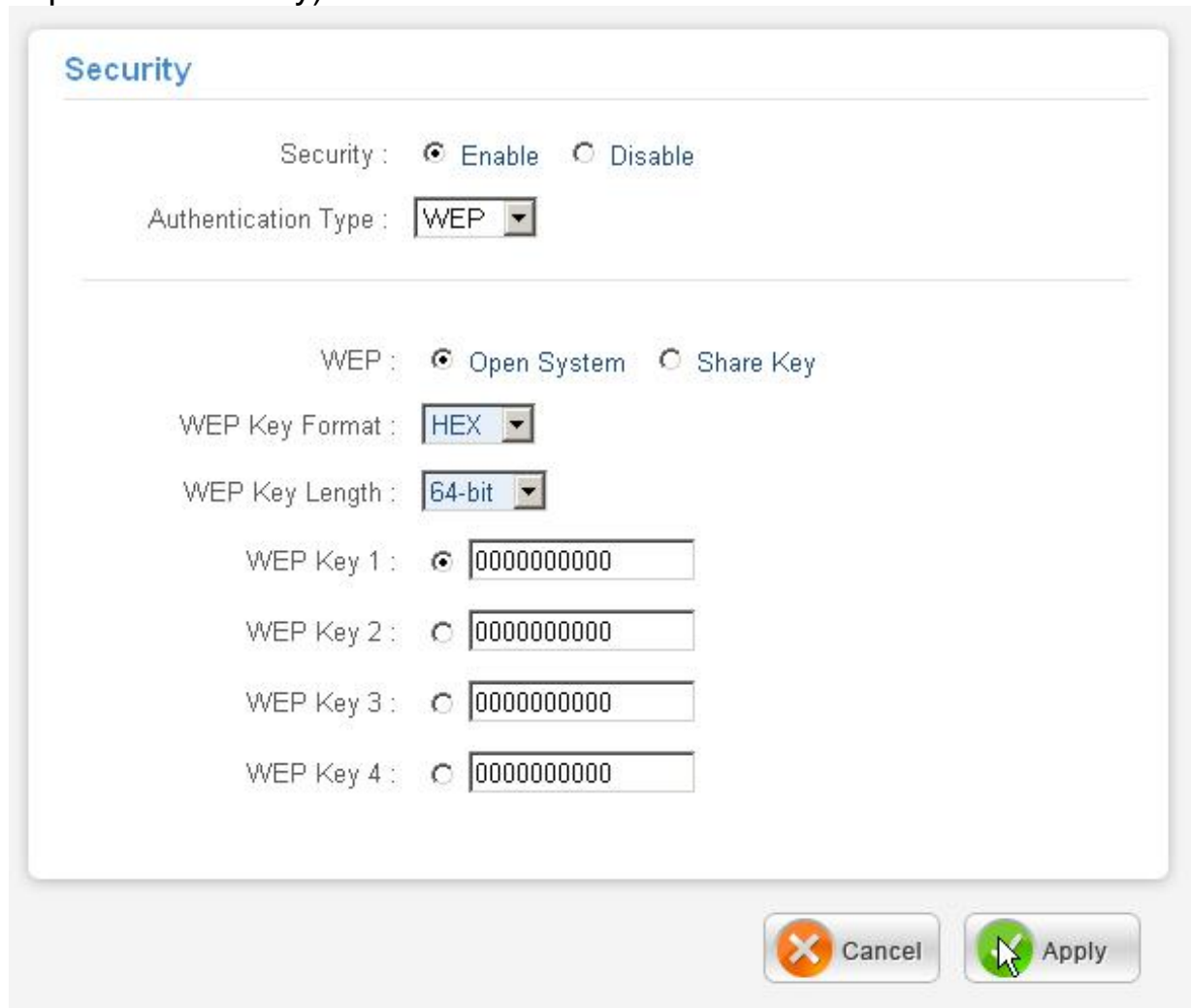
In questa sezione è possibile configurare le impostazioni di sicurezza legate all’interfaccia wireless dell’apparato.



Security: Cliccare **Enable** per abilitare la sicurezza sull’interfaccia Wireless.

Authentication Type: Selezionare la modalità di crittografia da utilizzare. E’ possibile scegliere tra: **WEP**, **WPA** o **WPA2**.

- **WEP:** Selezionare questa modalità per utilizzare l'algoritmo WEP (Wired Equivalent Privacy) con chiave statica a 64 o 128 bit.



Security

Security : Enable Disable

Authentication Type : WEP

WEP : Open System Share Key

WEP Key Format : HEX

WEP Key Length : 64-bit

WEP Key 1 : 0000000000

WEP Key 2 : 0000000000

WEP Key 3 : 0000000000

WEP Key 4 : 0000000000

Cancel Apply

WEP: Selezionare la modalità di negoziazione della chiave tra **Open System** o **Shared Key**.

WEP Key Format: Selezionare la modalità di immissione delle chiavi. Sono disponibili 2 scelte: **HEX** o **ASCII**.

WEP Key Length: Selezionare la lunghezza delle chiavi (64 o 128) dal menù a tendina.

WEP Key 1-4: Introdurre manualmente le 4 chiavi. Selezionare poi quale chiave utilizzare.

Cliccare su **Apply** per salvare le modifiche.

- **WPA/WPA2:** Selezionare questa modalità per utilizzare l'algoritmo WPA/WPA2 (Wi-Fi Protected Access).

Security

Security : Enable Disable

Authentication Type : WPA

Encryption Type : TKIP AES

PSK / EAP : PSK EAP

Passphrase :

Confirmed Passphrase :

Cancel
 Apply

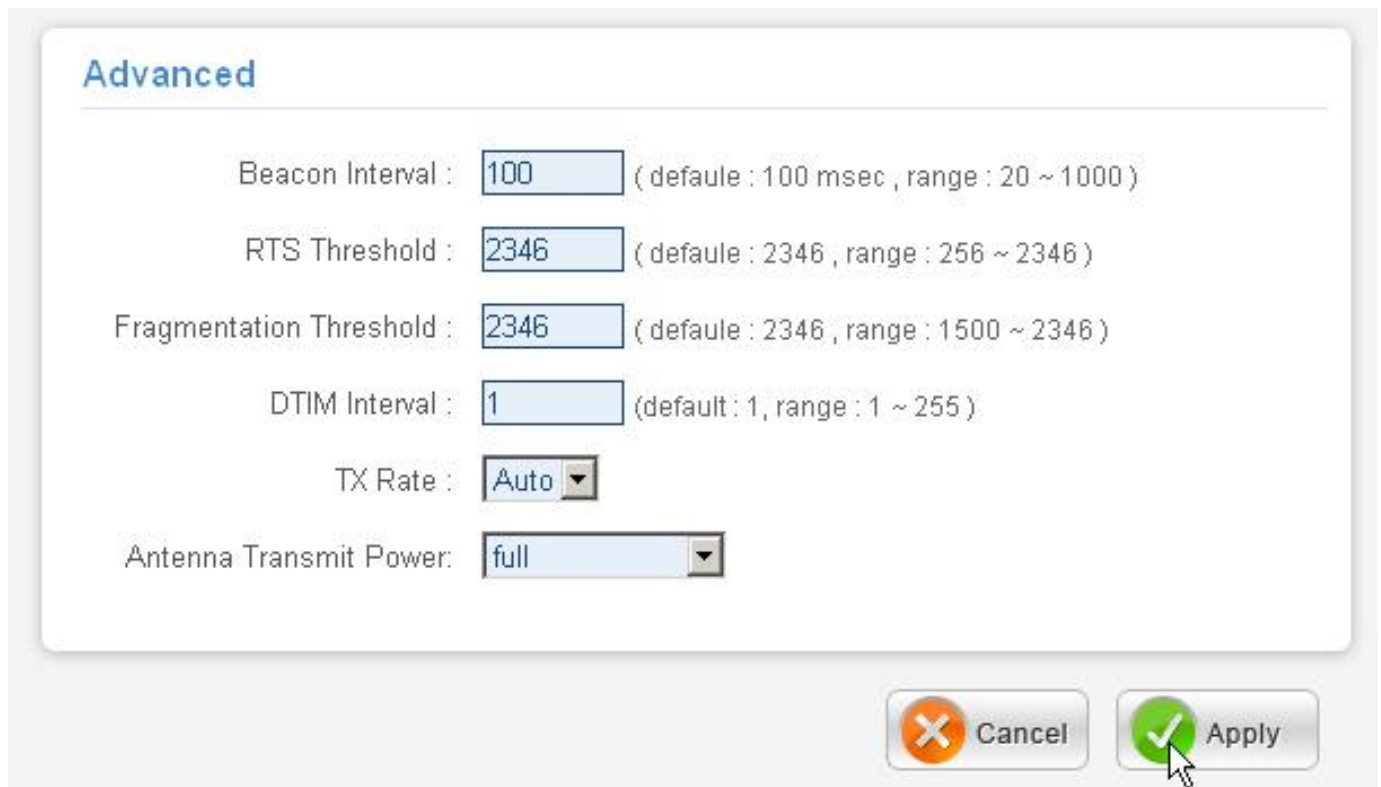
Encryption Type: Selezionare la modalità di cifratura tra **TKIP** o **AES**.
PSK / EAP: Selezionare la modalità di autenticazione tra **PSK** o **EAP** (la modalità EAP richiede un server RADIUS per l'autenticazione).

- **PSK**
Passphrase: Inserire la chiave precondivisa da utilizzare.
Confirmed Passphrase: Confermare la chiave immessa nel campo precedente.
- **EAP**
 Questa modalità richiede la presenza di un Radius Server per l'autenticazione dei client. Sarà necessario impostare l'IP del Radius, la porta di comunicazione e la chiave segreta condivisa.

Cliccare su **Apply** per salvare le modifiche.

3.5.3 Advanced

In questa sezione è possibile configurare tutti i dettagli della connessione wireless.



Advanced

Beacon Interval : (default : 100 msec , range : 20 ~ 1000)

RTS Threshold : (default : 2346 , range : 256 ~ 2346)

Fragmentation Threshold : (default : 2346 , range : 1500 ~ 2346)

DTIM Interval : (default : 1 , range : 1 ~ 255)

TX Rate :

Antenna Transmit Power:

Beacon Interval: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 100. L'intervallo permesso va da 20ms a 1000ms.

RTS Threshold: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 2436. L'intervallo permesso va da 256 sino a 2436. L'RTS (Request To Send) è un segnale, inviato dalla stazione trasmittente alla stazione ricevente, in cui si richiede il permesso per la trasmissione di dati.

Fragmentation Threshold: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 2346. L'intervallo permesso va da 256 sino a 2346. Cambiando tale valore le performance possono diminuire drasticamente.

DTIM Interval: Introdurre nell'apposito spazio il valore numerico riferito al DTIM (Delivery Traffic Indication Message). Il valore di default è 1. L'intervallo permesso va da 1 sino a 255.

TX Rates(MBps): E' possibile forzare la velocità (indicata in MegaBit al secondo) dell'apparato wireless, oppure lasciare su Auto.

Antenna Trasmit Power: E' possibile selezionare la potenza trasmissiva utilizzata nella trasmissione. Il valore di default è full. E' possibile scegliere tra **Full, Half, Quarter, Eight, Min.** Ogni valore dimezzera la potenza trasmissiva

rispetto a quello precedente, mentre **Min** regolerà la potenza in trasmissione al livello minimo.

Cliccare su **Apply** per salvare le modifiche.

3.6 LAN

3.6.1 Basic

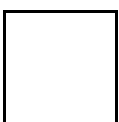
Questa sezione contiene i settaggi per la LAN interna.



Host Name: Inserire il nome del dispositivo.

IP Address/Subnet Mask: Questo è l'indirizzo IP con cui il Wireless Broadband Router è visto nella LAN (potrebbe essere un IP pubblico nel caso l'ISP fornisca una classe pubblica routata). E' necessario, qualora si cambiasse IP con quello di un'altra subnet accertarsi che tutti i PC della LAN abbiano un indirizzo IP (se non sono settati come client DHCP) nella stessa subnet. Diversamente questo potrebbe impedire il corretto funzionamento della LAN e l'accesso al Router.

Cliccare su **Apply** per salvare le modifiche.



Nel caso in cui l'IP del prodotto venga impostato su una classe di rete differente (es: 192.168.2.1), il DHCP provvederà ad adeguarsi alla nuova rete in maniera automatica.

3.6.2 DHCP

In questa sezione è possibile configurare i settaggi del DHCP Server integrato nel Wireless Broadband Router.



DHCP

DHCP Server : Enable Disable

DHCP Server Start IP :

DHCP Server End IP :

Lease Time :

DHCP Server: Sono disponibili 2 differenti opzioni:

- **Disable:** Selezionare per NON usare il DHCP Server nel Router che dunque non distribuirà gli indirizzi IP ai vari clients DHCP. In questo caso bisogna assegnare manualmente a tutti i PC della rete un indirizzo IP (diverso per ogni PC), la subnet mask, DNS e l'indirizzo del gateway (che, dovrebbe essere quello del Wireless Broadband Router nel caso sia usato in modalità Router, oppure del Router ADSL/ISDN nel caso in cui sia usato in modalità Access Point).
- **Enable:** Selezionare per usare il DHCP Server nel Router che dunque distribuirà gli indirizzi IP, subnet mask, gateway (l'indirizzo IP del Router) e DNS ai vari clients DHCP.

Start IP: Introdurre l'indirizzo IP di partenza del pool che il server DHCP assegnerà ai vari client. Il valore di default è: 192.168.1.100.

End IP: Introdurre l'indirizzo IP finale del pool che il server DHCP assegnerà ai vari client. Il valore di default è: 192.168.1.199.

Lease Time: Immettere il termine di scadenza scadenza dell'associazione IP fornita dal DHCP; al termine della stessa, il DHCP provvederà al rinnovo dell'IP associato al client..

Add Static DHCP

Static DHCP : Enable Disable

Name :

MAC address : - - - - -

IP address :

Static DHCP: Selezionare **Enable** nel caso in cui sia necessario associare in maniera statica un indirizzo IP ad un determinato MAC.

Name: Inserire il nome di identificazione dell'associazione statica che si sta immettendo.

MAC Address: Inserire il MAC Address al quale verrà associato staticamente l'indirizzo IP che verrà specificato nel campo **IP Address**.

IP Address: Inserire l'IP da associare staticamente al MAC Address specificato nel campo **MAC Address**.

Static DHCP List

Host Name	MAC Address	IP Address
-----------	-------------	------------

Dynamic DHCP List

Host Name	MAC Address	IP Address	Expired Time
unknown	00-e0-18-df-7b-64	192.168.1.127	Apr/08/2002 00:00:00

Nelle tabelle **Static DHCP List** e **Dynamic DHCP List** è possibile verificare le associazioni, statiche e dinamiche, del DHCP Server.

Nella tabella **Dynamic DHCP List** sarà quindi possibile visualizzare i client connessi al Wireless Broadband Router, mentre le associazioni presenti nella **Static DHCP List** rimarranno visibili anche se il client interessato non è connesso al prodotto.



3.7 Access Control

Questa sezione contiene i settaggi relativi al NAT e al Firewall del Wireless Broadband Router.

3.7.1 Filter

In questa sezione è possibile configurare diversi tipi di filtraggio sul traffico proveniente dalla LAN verso l'interfaccia WAN.

E' possibile selezionare tra **MAC Filters**, **IP Filters**, **URL Blocking**, **Domain Blocking** e **Protocol Filters**.

Filters

Filters are used to allow or deny LAN users from accessing the Internet.

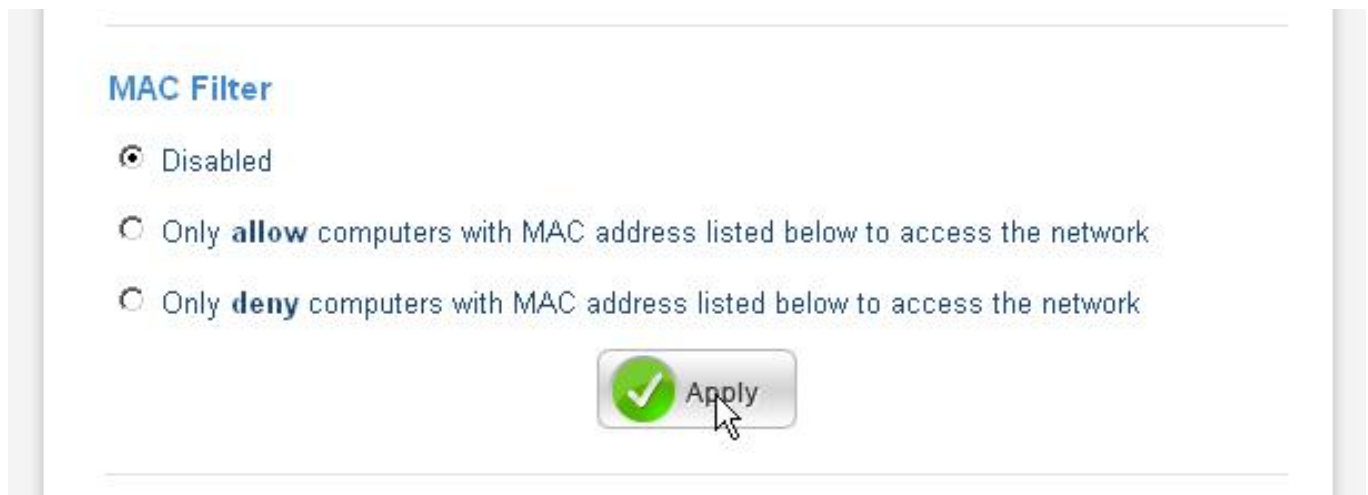
- MAC Filters
- IP Filters
- URL Blocking
- Domain Blocking
- Protocol Filters

3.7.1.2 MAC Filter

Questa sezione permette di configurare il Wireless Broadband Router in modo da fornire l'accesso solo dopo aver controllato il MAC address del client wireless.

E' possibile pertanto permettere:

- l'accesso ad una lista esclusiva di MAC address (selezionare **Only allow computers with MAC address listed below to access the network**)
- l'accesso a tutti e bloccare una lista di MAC address ben precisa (selezionare **Only deny computers with MAC address listed below to access the network**).



MAC Filter

Disabled

Only **allow** computers with MAC address listed below to access the network

Only **deny** computers with MAC address listed below to access the network

Cliccare su **Apply** per salvare le modifiche.

Nel caso si sia scelto di attivare questa funzionalità, sarà ora necessario inserire una lista di indirizzi MAC da bloccare o a cui permettere l'accesso.

MAC Table

Name :

MAC Address : - - - - -

Name	MAC Address
------	-------------

Name: Introdurre un identificativo.

MAC Address: Introdurre l'indirizzo MAC

Add: Cliccare per aggiungere l'utente alla lista

Update: Se si cambia un campo, cliccare su Update per aggiornare la tabella

Delete: Selezionare un utente dalla tabella e cancellarlo premendo il tasto **Delete**

Clear: Ripulisce tutti i campi dai valori immessi

3.7.1.3 IP Filter

E' possibile filtrare l'accesso ad Internet utilizzando come criterio l'indirizzo IP di sorgente.

IP Filter

Enabled : Enable Disabled

Range Start :

Range End :

	Start	End

Enable/Disable: Abilita o disabilita il filtraggio per indirizzo IP

Range Start/Range End: Inserire rispettivamente il primo e l'ultimo indirizzo IP da filtrare. (nel caso si tratti di un IP singolo, nella tabella sottostante verrà riportato il solo valore **Start** mostrante l'IP immesso).

Add: Cliccare per aggiungere un filtro alla lista

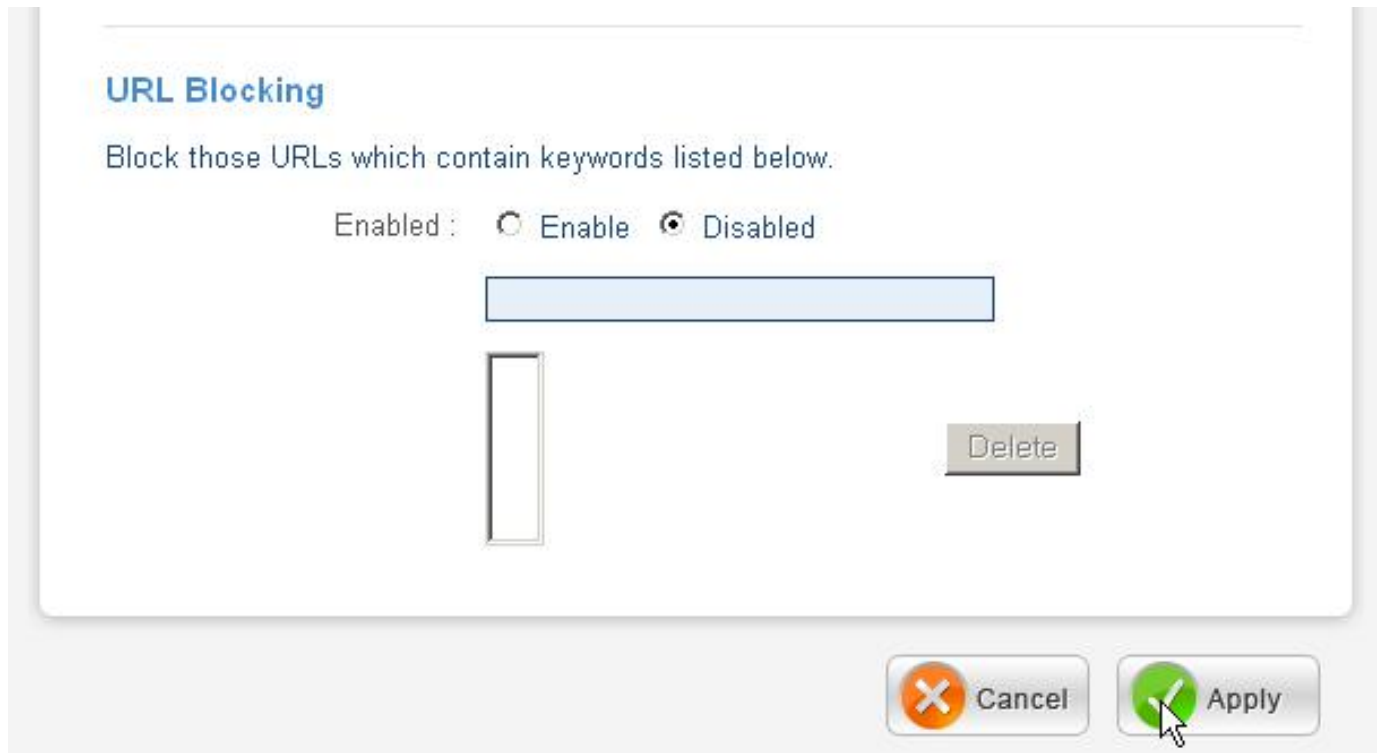
Update: Se si cambia un campo, cliccare su Update per aggiornare la tabella

Delete: Selezionare un filtro dalla tabella e cancellarlo premendo il tasto **Delete**

Clear: Ripulisce tutti i campi dai valori immessi

3.7.1.4 URL Blocking

E' possibile filtrare l'accesso ad alcuni siti utilizzando come criterio alcune parole contenute nel nome del dominio.



URL Blocking

Block those URLs which contain keywords listed below.

Enabled : Enable Disabled

Delete

Cancel Apply

Enable/Disabled: Abilita o disabilita la funzione di filtraggio delle URL. Non appena attivata, inserire nella textbox sottostante la parola che si decide di utilizzare come criterio di filtraggio. Cliccare su **Apply** per aggiungere la parola tra lista delle parole “vietate” che il Wireless Broadband Router bloccherà se presenti nel nome del dominio che si cercherà di contattare.

Delete: Selezionare la parola che si intende rimuovere dalla lista e premere questo tasto per eliminarla.

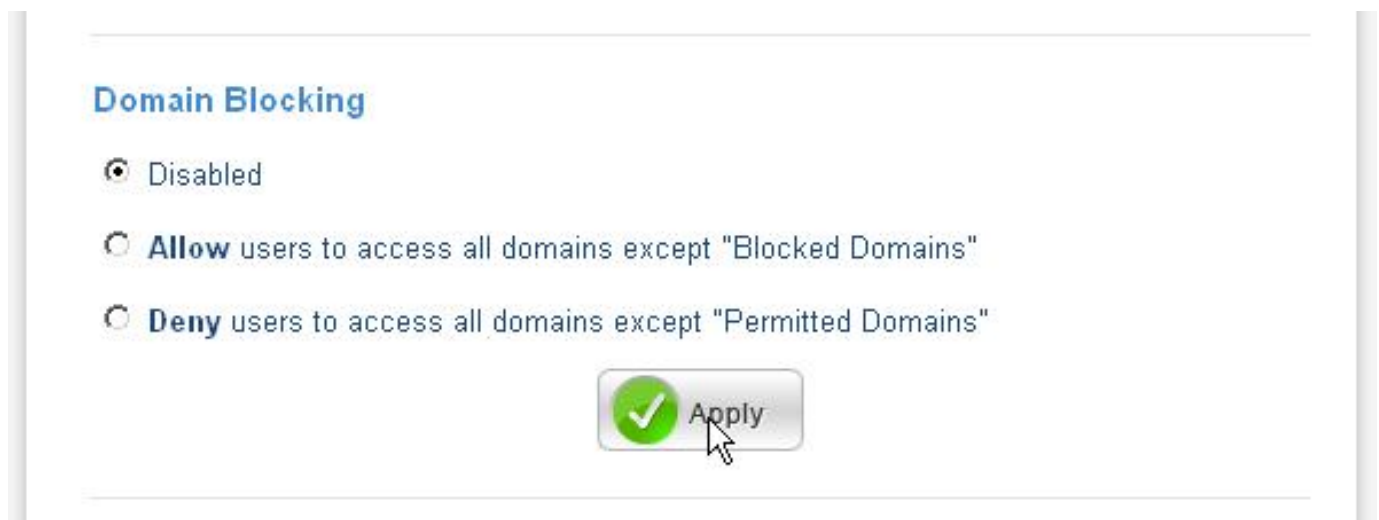
3.7.1.5 Domain Blocking

E' possibile filtrare l'accesso ad alcuni siti utilizzando come criterio di filtraggio il dominio del sito stesso.

E' possibile pertanto:

- Permettere l'accesso a tutti i domini tranne quelli contenuti nella lista "Blocked Domains" (selezionare **Allow users to access all domains except "Blocked Domains"**)
- Bloccare l'accesso a tutti i domini tranne quelli contenuti nella lista "Permitted Domains" (selezionare **Deny users to access all domains except "Permitted Domains"**).

Cliccare su **Apply** per salvare le modifiche.



Selezionando l'opzione, apparirà una sezione dove inserire i domini permessi o quelli da bloccare.

Per inserire un dominio, compilare la textbox e premere **Add** per aggiungerlo alla lista sottostante. Per rimuovere un dominio dalla lista, selezionarlo e premere il tasto **Del**.

3.7.1.6 Protocol Filter

E' possibile filtrare l'utilizzo di alcuni protocolli, tra i quali HTTP, HTTPS, FTP, Telnet, SMTP e POP3.

Protocol Filter

Disabled
 Enabled :Deny to access internet from LAN when the list as below item be enable.

Edit Protocol Filter in List

Enabled : Enable Disabled

Name :

Protocol : ▾

Port : -

	Name	Protocol	Range
<input type="checkbox"/>	Filter FTP	TCP	20-21
<input type="checkbox"/>	Filter HTTP	TCP	80
<input type="checkbox"/>	Filter HTTPS	TCP	443
<input type="checkbox"/>	Filter DNS	UDP	53
<input type="checkbox"/>	Filter SMTP	TCP	25
<input type="checkbox"/>	Filter POP3	TCP	110
<input type="checkbox"/>	Filter Telnet	TCP	23

Selezionare **Enabled** per abilitare la funzione e premere **Apply**.

Verrà visualizzata una lista preimpostata di filtri sui servizi più conosciuti (FTP, HTTP, HTTPS, DNS, SMTP, POP3, Telnet).

Selezionare **Enable** per attivare la regola che si sta creando e immettere i dati:

Name: Inserire il nome della regola

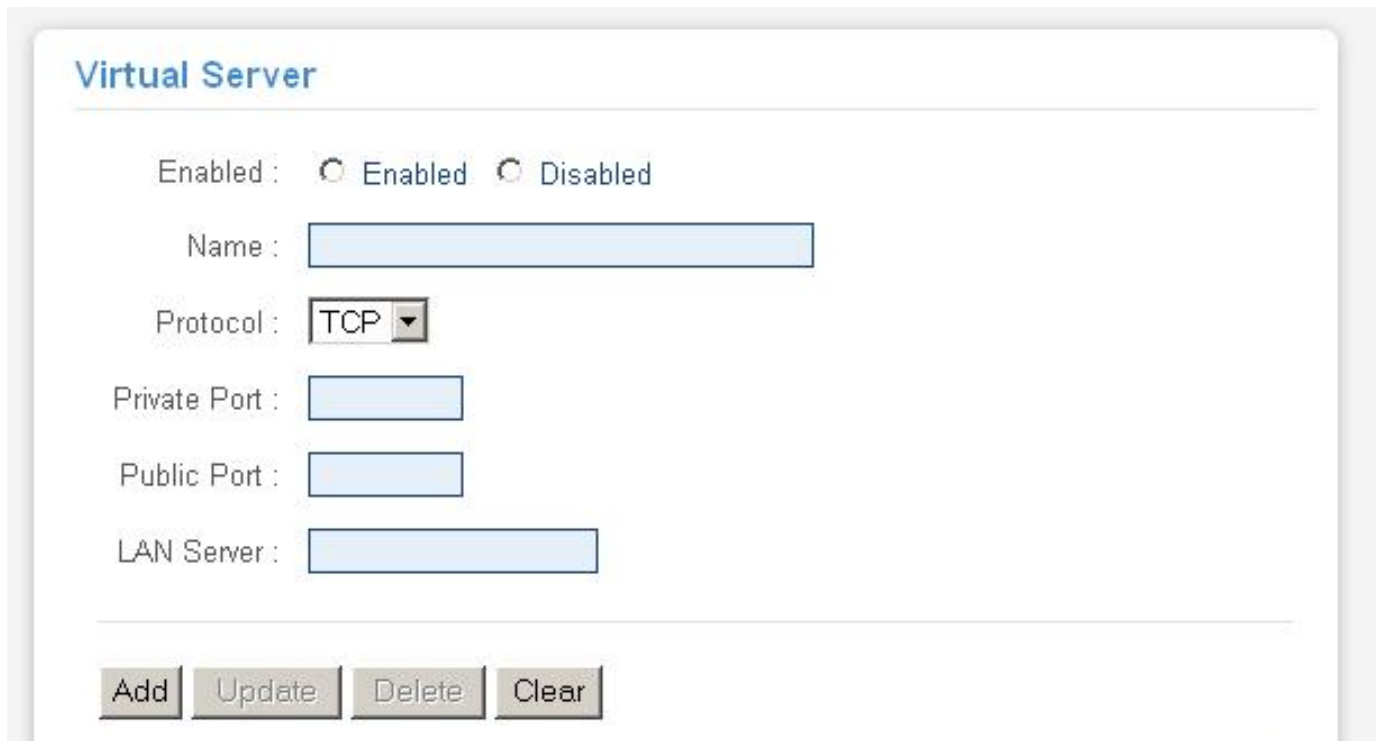
Protocol: Selezionare il tipo di protocollo tra TCP, UDP o *.

Port: Immettere il numero di porta o il range di porte da filtrare.

E' inoltre possibile modificare la lista preimpostata; basterà selezionare una voce dalla lista evidenziandola e cliccare su **Enable** per attivarla. Una volta modificata, premere sul tasto **Update** per salvare le modifiche.

3.7.2 Virtual Server

Il Firewall/Nat del Wireless BroadBand Router consente la protezione della LAN locale da parte di accessi indesiderati. Può essere necessario, consentire ad utenti esterni l'accesso ad un PC specifico della Lan (per esempio verso un PC fa da server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta (si ricorda che Web =80, FTP =20/21, Telnet =23, SMTP =25, POP3 =110, DNS =53, ECHO =7, NNTP =119) , su un PC della Lan interna. E' possibile scegliere la porta ed il protocollo (tra TCP,UDP o entrambi) che si intende rigirare sull'indirizzo IP.



The screenshot shows the 'Virtual Server' configuration page. At the top, the title 'Virtual Server' is displayed in blue. Below the title, there are several configuration fields: 'Enabled' with radio buttons for 'Enabled' and 'Disabled'; 'Name' with a text input field; 'Protocol' with a dropdown menu currently set to 'TCP'; 'Private Port' with a text input field; 'Public Port' with a text input field; and 'LAN Server' with a text input field. At the bottom of the form, there are four buttons: 'Add', 'Update', 'Delete', and 'Clear'.

Enabled: Abilita o disabilita la funzionalità la regola selezionata o che si sta creando.

Name: Inserire il nome identificativo della regola che si sta creando o che si selezionato dall'elenco di regole preconfigurate

Protocol: Selezionare il tipo di protocollo (scegliere tra TCP, UDP o entrambi)

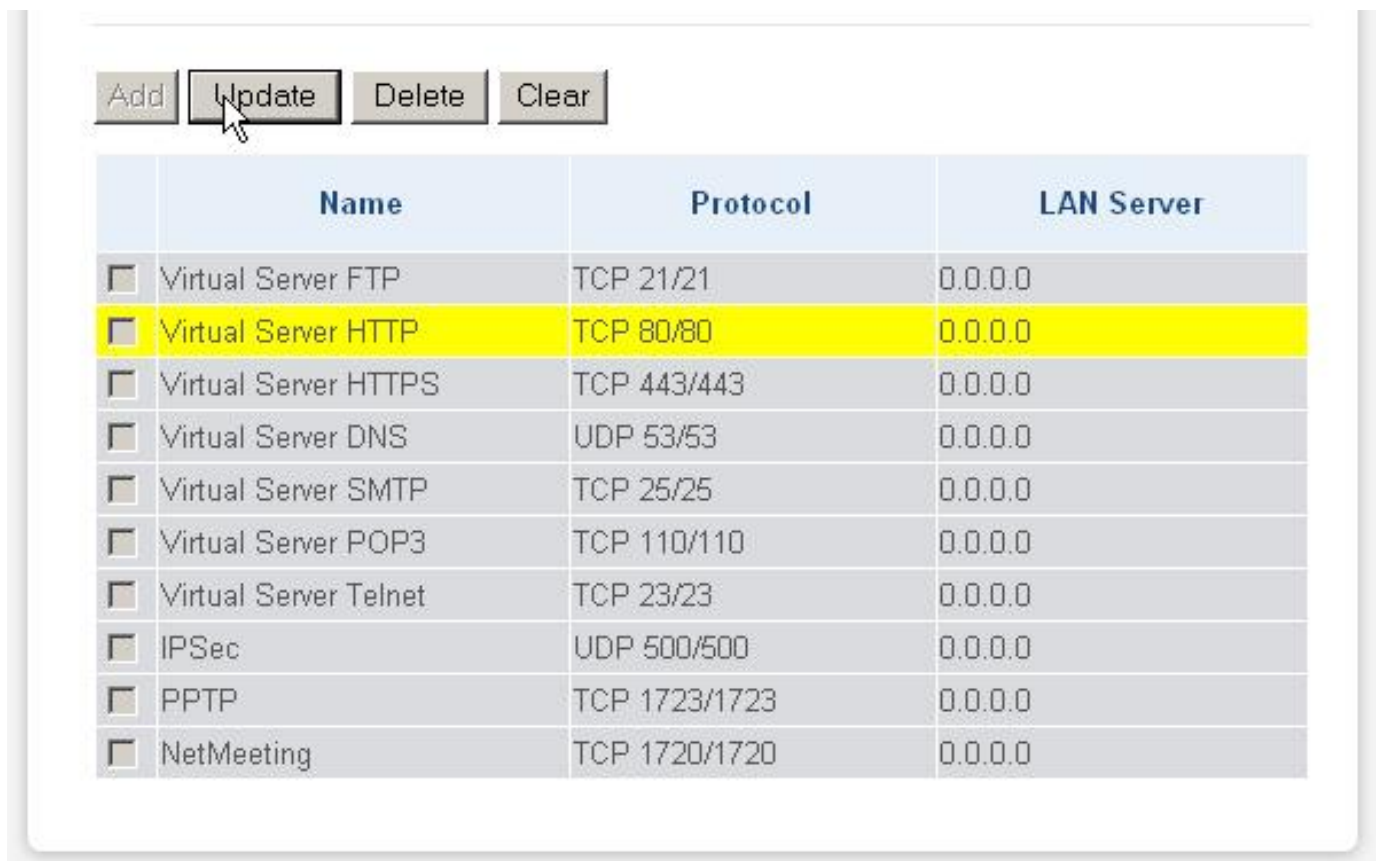
Private Port: Inserire il numero di porta (compreso tra 0-65535)

Public Port: Inserire il numero di porta (compreso tra 0-65535)

LAN Server: Inserire l'indirizzo IP su cui è necessario reindirizzare il servizio

La sezione Firewall viene prima di quella del Virtual Server, assicurarsi che le porte/protocolli ruotati non siano bloccati dal Firewall.

Sono anche presenti tutta una serie di Virtual Server preconfigurati, come da figura:



The screenshot shows a web interface for configuring Virtual Servers. At the top, there are four buttons: 'Add', 'Update', 'Delete', and 'Clear'. Below the buttons is a table with the following columns: 'Name', 'Protocol', and 'LAN Server'. The table lists several pre-configured services, with 'Virtual Server HTTP' highlighted in yellow.

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTP	TCP 80/80	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	IPSec	UDP 500/500	0.0.0.0
<input type="checkbox"/>	PPTP	TCP 1723/1723	0.0.0.0
<input type="checkbox"/>	NetMeeting	TCP 1720/1720	0.0.0.0

Se sul Wireless Broadband Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual

Server per evitare conflitti. In questo caso è sufficiente assegnare al Virtual Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Wireless Broadband Router) ed i server DNS) un indirizzo IP che sia nella stessa subnet del Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router.

Se per esempio il server WEB (che riceverà chiamate sulla porta 80) della LAN ha indirizzo IP privato 192.168.1.127 anzitutto è necessario evidenziare nella tabella il servizio opportuno. Poi abilitarlo (spuntando **enable**, configurarlo mettendo l'IP 192.168.1.2 ed infine validarlo premendo **update**). Il risultato finale dovrebbe essere come in figura sotto.

E' chiaro che in questo caso non dovremo utilizzare il DHCP client sul PC poichè in tal caso non conosceremo l'IP che il server Web potrebbe prendere.

E' importante sapere che il Wireless Broadband Router esegue, in ordine di numerazione crescente, le associazioni richieste dai vari Virtual Server e solo alla fine (qualora fosse presente) rigira il tutto alla DMZ. Pertanto se la porta (20)21 è mappata (ad esempio) su un certo PC della rete tramite Virtual Server, il PC il cui indirizzo è indicato nel DMZ non potrà funzionare come server FTP.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del Router. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consultare eventuali aggiornamenti di questo manuale.

Applicazione	Settaggi connessioni Uscenti	Settaggi connessioni Entranti
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
MIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey	Nessuno	principalmente 4660-4662 TCP , 4665 UDP
MSN Messenger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863, 6901 e 5190

Usando NetMeeting (Versione3.0), ad esempio, quando la chiamata generata è uscente da un PC dietro al Router verso un PC esterno non ci sono problemi. Il contrario non è realizzabile. Rigirando invece le porte 1503(TCP) e 1720(TCP) è possibile ricevere anche chiamate in ingresso con video (h.323 e T.120). In figura è presente una configurazione di VS per ricevere chiamate in ingresso in Netmeeting (vengono rigirate al PC con IP 192.168.2.100).

Attenzione il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range (o centinaia di connessioni contemporanee) potrebbero sorgere problemi derivanti dal limite fisico della memoria allocabile dal processo NAT.

Sono allegate tutta una serie di porte notevoli (da utilizzarsi per il VS ed il Firewall):



Servizio	Numero di Porta / Protocollo
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

3.7.3 Special AP

E' possibile abilitare particolari applicazioni, come i videogames, che richiedono connessioni multiple (generalmente critiche quando si usa il NAT). Sono già contenuti tutta una serie di settaggi per i videogames/applicazioni più comuni.

Special AP

Enabled : Enabled Disabled

Name :

Trigger

Protocol : ▼

Port Range : -

Incoming

Protocol : ▼

Port :

	Name	Trigger	Incoming
<input type="checkbox"/>	Battle.net	* 6112	* 6112

Enable: Per abilitare il servizio.

Name: Tipo descrittivo dell'applicazione.

Trigger: Definisce le porte e protocolli delle comunicazioni uscenti che determinano poi le porte ed i protocolli di comunicazioni entranti.

- **Protocol:** Selezionare tra TCP, UDP oppure ICMP.
- **Port Range:** Selezionare l'intervallo di porte usato dall'applicazione

Incoming: Definisce l'intervallo di porte da aprire in risposta alla comunicazione uscente.

- **Protocol:** Selezionare l'intervallo di porte usato dall'applicazione.
- **Port:** Selezionare l'intervallo di porte usato dall'applicazione.

Add: Cliccare per aggiungere un nuovo profilo alla tabella.

Update: Se si cambia un campo, cliccare su Update per aggiornare la tabella.


Delete: Selezionare un profilo dalla tabella e cancellarlo premendo il tasto.

New: Per cancellare tutti i campi.

E' possibile, selezionare dalla lista già presente, abilitare/disabilitare il servizio e poi premere su **Update**.

3.7.4 DMZ

E' a tutti gli effetti un computer esposto ad Internet, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server).



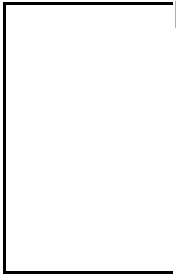
Enabled: Per abilitare la funzionalità DMZ.

DMZ Host IP: Indicare l'indirizzo IP della macchina sulla quale verrà indirizzato tutto il traffico entrante.

Cliccare su **Apply** per salvare le modifiche.



In questo modo l'indirizzo IP è completamente esposto.



3.7.5 Firewall Rule

Queste funzioni di filtraggio dei pacchetti IP sono in buona sostanza una serie di regole che il Router applicherà ai pacchetti IP che lo attraversano e stabilirà o meno il soddisfacimento di queste regole, pacchetto per pacchetto. E' utile comunque sapere che il solo filtraggio sui pacchetti non elimina i problemi legati a livello di applicazione o altri livelli.

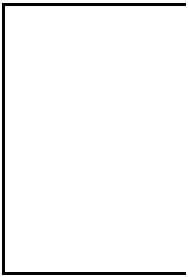
Le politiche con cui organizzare un filtraggio sono essenzialmente riassumibili in due posizioni:

- **Blocco ciò che conosco come pericoloso e consento il passaggio del resto:** Tale posizione dovrebbe essere applicata da coloro che possiedono una discreta conoscenza di Internet. Richiede la conoscenza dei pericoli da filtrare opportunamente e consente, nella maggior parte dei casi, di non imbattersi in decine di applicazioni che hanno problemi perché mal configurate (con questa filosofia si blocca solo il pericolo).
- **Passa solo quello che ritengo sicuro il resto è bloccato:** Tale posizione dovrebbe essere applicata da coloro che possiedono una buona conoscenza di Internet in quanto è necessario creare una regola per ogni "servizio" che si vuole usare. E' certamente più sicura ma richiede una maggiore conoscenza delle problematiche ed una più lunga preparazione delle regole dei filtri (che possono essere moltissimi).

Una volta realizzate le regole che determinano il modo in cui avviene il filtraggio dei pacchetti IP è opportuno verificare la sicurezza del sistema. Questo è realizzabile in diverse modalità:

- **Sito specializzato:** In questo caso è possibile ottenere un primo risultato visitando il sito <http://www.dslreports.com> (ve ne sono ovviamente moltissimi altri) e accedendo alla sezione DSLR Tools ed infine scegliere Port-Scan. I risultati possibili, per ogni porta controllata, possono essere 3 (open: la porta è in ascolto e dietro c'è un servizio che accetta le connessioni, closed: la porta rifiuta la connessione e non è dato sapere se c'è un servizio dietro, stealth: la porta non risponde alla richiesta di connessione)
- **PC esterno alla LAN:** In questo modo potete provare le politiche di filtraggio.

Il modulo Virtual Server è sincronizzato con Firewall. Ogni impostazione del Virtual Server viene immediatamente replicata nel Firewall.



Le regole vengono eseguite dall'alto verso il basso. Più in alto è una regola, prima sarà eseguita.



Vediamo adesso come configurare il Firewall.

Firewall Rule

Enabled : Enabled Disabled

Name :

Action : Allow Deny

Source :

Interface IP Range Start IP Range End

Destination :

Interface IP Range Start IP Range End Protocol Port Range
 -

	Action	Name	Source	Destination	Protocol
<input checked="" type="checkbox"/>	Allow	Allow to Ping WAN port	WAN,*	WAN,*	ICMP,
<input checked="" type="checkbox"/>	Deny	Default	WAN,*	LAN,*	*,*
<input checked="" type="checkbox"/>	Allow	Default	LAN,*	WAN,*	*,*

Enable/Disable: Per abilitare o disabilitare la singola regola.

Name: Introdurre un identificativo

Action: Selezionare l'azione una volta che la regola è soddisfatta. **Allow** inoltra il pacchetto, **Deny** lo scarta.

Source: Definisce la sorgente dei pacchetti. Potrete scegliere tra WAN o LAN.

- **Interface:** Selezionare l'interfaccia (WAN oppure LAN) cui la regola è applicata.
- **IP Range Start:** Introdurre l'indirizzo IP di partenza. Usare l'asterisco(*) per includere ogni IP.
- **IP Range End:** Introdurre l'indirizzo IP finale.

Destination: Definisce la destinazione dei pacchetti. Potrete scegliere tra WAN o LAN.

- **Interface:** Selezionare l'interfaccia (WAN oppure LAN) cui la regola è applicata.
- **IP Range Start:** Introdurre l'indirizzo IP di partenza. Usare l'asterisco(*) per includere ogni IP.
- **IP Range End:** Introdurre l'indirizzo IP finale.
- **Protocol:** Selezionare il protocollo (ICMP, UDP, TCP o tutti)
 - **TCP** (Transmission Control Protocol): Tale protocollo fornisce un servizio di comunicazione basato sulla connessione (al contrario dell'IP e UDP). Tale servizio è affidabile. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). E' usato moltissimo specie per Telnet (porta 23), FTP (porta 20 e 21), http (porta 80), SMTP e POP3 (porta 25 e 110).
 - **UDP** (User Datagram Protocol): Tale protocollo fornisce un servizio di comunicazione non basato sulla connessione (come dell'IP). Tale servizio è più veloce del TCP sebbene meno sicuro. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). E' utilizzato per interrogare i DNS.
 - **ICMP** (Internet Control Message Protocol): Viene usato per notificare al mittente eventuali problemi legati ai datagrammi IP. I principali messaggi dell'ICMP sono: Destination Unreachable (l'host non è raggiungibile e pertanto il pacchetto non sarà consegnato), Echo Reply ed Echo Request (usati per verificare la raggiungibilità di alcuni host nella rete), Parameter Problem (indica che un Router che ha esaminato il pacchetto ha rilevato un qualche problema nell'intestazione), Redirect (usato da un host o un Router per avvisare il mittente che i pacchetti dovrebbero essere inviati ad un altro indirizzo), Source Quench (inviato da un Router congestionato al mittente per informarlo dello stato), Timestamp e Timestamp Reply (simili ai messaggi di Echo, ma aggiungono l'orario) TTL Exceeded (il campo TTL è sceso a zero, dunque il pacchetto è stato scartato e ne viene informato il mittente).
- **IP Range Start:** Introdurre l'indirizzo IP di partenza. Usare l'asterisco(*) per includere ogni IP.

Add: Cliccare per aggiungere un nuovo profilo alla tabella di regole

Update: Se si cambia un campo, cliccare su Update per aggiornare la tabella

Delete: Selezionare un profilo dalla tabella e cancellarlo premendo il tasto

New: per cancellare tutti i campi

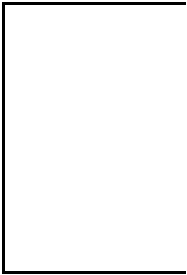
Priority Up: Scegliere una regola dalla lista e cliccare su Priority Up per incrementarne la priorità.



Priority Down: Scegliere una regola dalla lista e cliccare su Priority Down per diminuirne la priorità.

Update Priority: Cliccare solo dopo aver modificato la priorità. Vedrete la regola spostarsi di conseguenza.

Le regole create dalle funzioni di Filter, Virtual Server o DMZ non sono direttamente modificabili. Fare riferimento all'apposita sezione di configurazione delle singole funzionalità per apportare delle modifiche sulle stesse.

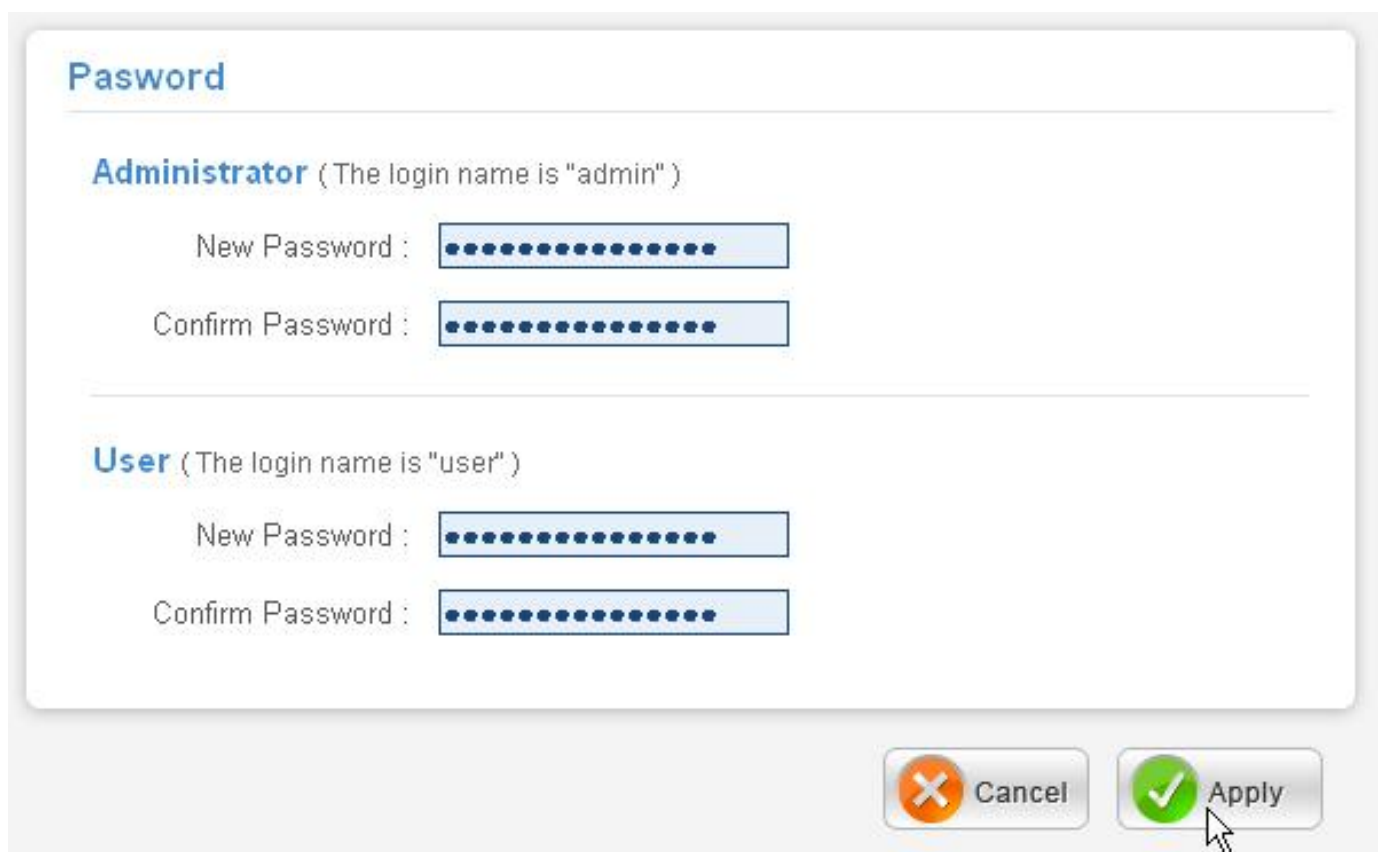


3.8 System

3.8.1 Password

In questa sezione è possibile configurare le password di accesso dell'apparato. E' estremamente importante sostituire la password di accesso al Wireless Broadband Router per incrementare il livello di sicurezza del dispositivo. In questa sezione sarà possibile reimpostare la password di amministratore (admin) e quella utente (user).

Introdurre la nuova password in **New Password** e poi per conferma in **Confirm Password**. La password può essere composta al massimo da 16 caratteri alfanumerici.



The screenshot shows a web interface titled "Pasword" (sic) for configuring passwords. It is divided into two sections: "Administrator" and "User".

Administrator (The login name is "admin")

New Password :

Confirm Password :

User (The login name is "user")

New Password :

Confirm Password :

At the bottom right, there are two buttons: "Cancel" (with a red 'X' icon) and "Apply" (with a green checkmark icon). A mouse cursor is pointing at the "Apply" button.

Cliccare poi su **Apply** per rendere operativa la nuova password di accesso.



E' possibile, qualora si dimenticasse la password di accesso del dispositivo, resettarlo premendo l'apposito bottone (per almeno 10 secondi) posto sul retro. A questo punto verrà caricato il firmware con le impostazioni di default (username=**admin**, password=**admin**).

3.8.2 Time

Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente.

Time

Local Time : Apr/01/2002 02:40:31

Time Zone : (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Time Setting

Synchronize the Clock with NTP Server : Enable Disable

NTP Server : (default)

Manually Date and Time Setting

2002 Month Apr Day 01 Hour 02 Minute 40 Second 31

Daylight Saving

Daylight Saving : Enabled Disabled

Start Jan 01 End Jan 01

Local Time: Viene mostrata l'ora

Time Zone: Per scegliere la zona di appartenenza sarà sufficiente selezionare il fuso di appropriato; selezionare poi **Enable** sul campo Synchronize the Clcck with NTP Server ed inserire l'indirizzo di un server NTP nel campo NTP Server.

NTP Server: Introdurre l'indirizzo IP del server opportuno.

Manually Date and Time Setting: Per introdurre manualmente l'ora. Cliccare poi su **Set Time** per salvare le nuove impostazioni orarie.

Daylight Saving: Scegliere **Enable** e immettere il periodo entro cui è ... l'ora legale.

Cliccare poi su **Apply** per salvare le modifiche.

3.8.3 Device Information

In questa sezione è possibile conoscere i dettagli relativi all'interfaccia WAN, LAN e WLAN.

La sezione è suddivisa in **WAN**, **Wireless**, **LAN** e **DHCP Client List**..

- **WAN:** Visualizza tutti i parametri relativi all'interfaccia WAN.



The screenshot shows the 'Device Information' page with the 'WAN' tab selected. The settings are as follows:

MAC Address :	00-18-e7-11-44-73
Connection Type :	DHCP Client Disconnected
	<input type="button" value="DHCP Release"/> <input type="button" value="DHCP Renew"/>
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0
DNS :	

- **Wireless:** Visualizza tutti i parametri relativi all'interfaccia WLAN



Wireless

Connection : 802.11g AP Enable

SSID : default

Channel : 6

Antenna Power : Full

Authentication Type : Disabled

Wireless Client List :

- **LAN:** Visualizza tutti i parametri relativi all'interfaccia LAN.

LAN

MAC Address : 00-18-e7-11-44-72

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server : Enabled

[DHCP Client List](#)

Connected Time	MAC Address	Mode
----------------	-------------	------

Nella sezione **DCHP Client List** sarà possibile visualizzare una lista dei client che sono associati al Wireless Broadband Router e che hanno fatto richiesta al DHCP Server integrato del prodotto.

3.8.4 Log

Il Router mostra tutti gli ultimi 200 Log (i più vecchi saranno sovrascritti dai più recenti).

Cliccando nei bottoni, nella parte superiore, è possibile rapidamente fare scorrere tutte le pagine dei vari log. Con **Clear Log** la memoria dei Log verrà cancellata e con **Refresh** è possibile ottenere un aggiornamento istantaneo.

Log

Page 1 of 4

First Page
Last Page
Previous Page
Next Page
Clear Log

Refresh

Time	Message	Source	Destination	Note
Apr/01/2002 00:02:36	DHCP Discover			
Apr/01/2002 00:02:34	DHCP Discover			

Time: Mostra la data e l'ora di creazione del log

Message: Mostra la tipologia del log

Source: Indica la sorgente della comunicazione

Destination: Indica la destinazione

Note: Viene mostrato l'indirizzo IP della destinazione

3.8.5 Log Settings

E' possibile configurare tutti i parametri relativi alla gestione dei Log.

Log Setting

SMTP Authentication : Enabled Disabled

SMTP Account :

SMTP Password :

SMTP Server / IP Address :

Send From : (email address)

Send to : (email address)

Syslog Server :

Log Type

- System Activity
- Debug Information
- Attacks
- Dropped Packets
- Notice



SMTP Authentication: Scegliere **Enabled** per utilizzare la funzione di segnalazione via email.

SMTP Account: Introdurre l'account per l'autenticazione sul server SMTP dell'ISP affinché il Router possa inviare all'indirizzo mail, contenuto nel campo **Send to**, tutti i dettagli relativi ai Log.

SMTP Password: Introdurre la password per l'autenticazione sul server SMTP dell'ISP dell'account inserito nel campo **SMTP Account**.

SMTP Server / IP Address: Introdurre il nome o l'indirizzo IP del server SMTP da utilizzare.

Send from: Introdurre l'indirizzo mail con cui inviare i Log.

Send to: Introdurre l'indirizzo mail cui inviare i Log. Cliccando su **Email Log Now** effettuerete un invio immediato.

Syslog Server: Introdurre l'indirizzo IP del server SysLog cui il Router invierà il dettaglio dei Log. In questa maniera è possibile controllare puntualmente e senza limite alcuno il dispositivo (grazie all'utilizzo di un server Syslog esterno residente su una macchina).

Log Type: Selezionare i contenuti del Log

- **System Activity:** Mostra le informazioni relative all'attività dell'apparato.
- **Debug Information:** Mostra le informazioni circa il corretto caricamento dei moduli dell'apparato.
- **Attacks:** Mostra informazioni circa qualsiasi attività sospetta.
- **Dropped Packets:** Mostra informazioni sui pacchetti che non sono trasferiti con successo.
- **Notice:** Notizie riservate all'amministratore


Cliccare poi su **Apply** per salvare le modifiche.

3.8.6 Statistics

In questa sezione è possibile conoscere i dettagli relativi all'interfaccia WLAN e WAN. Vengono mostrate le informazioni relative al numero di pacchetti spostati.

Statistic

Utilization (bytes/sec)		LAN	WAN	Wireless
Send	Average :	16	0	1
	Peak :	120	0	1
Receive	Average :	27	0	0
	Peak :	171	0	0



Cliccare su **Reset** per azzerare le statistiche.

3.8.7 Restart

Premere sul pulsante Restart per riavviare il prodotto mantenendo le configurazioni salvate.

3.8.8 Firmware

In questa sezione è possibile visualizzare la versione di firmware caricata sul Wireless Broadband Router ed effettuare l'aggiornamento dello stesso.



Firmware Version: Mostra la versione di firmware correntemente utilizzata dal Wireless Broadband Router.

Upgrade Firmware: E' possibile effettuare l'upgrade del firmware del dispositivo. Seguire le seguenti istruzioni :

- Scaricare l'ultimo firmware dal sito www.atlantis-land.com
- Cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file precedentemente scaricato, e cliccare poi su **Upgrade**.

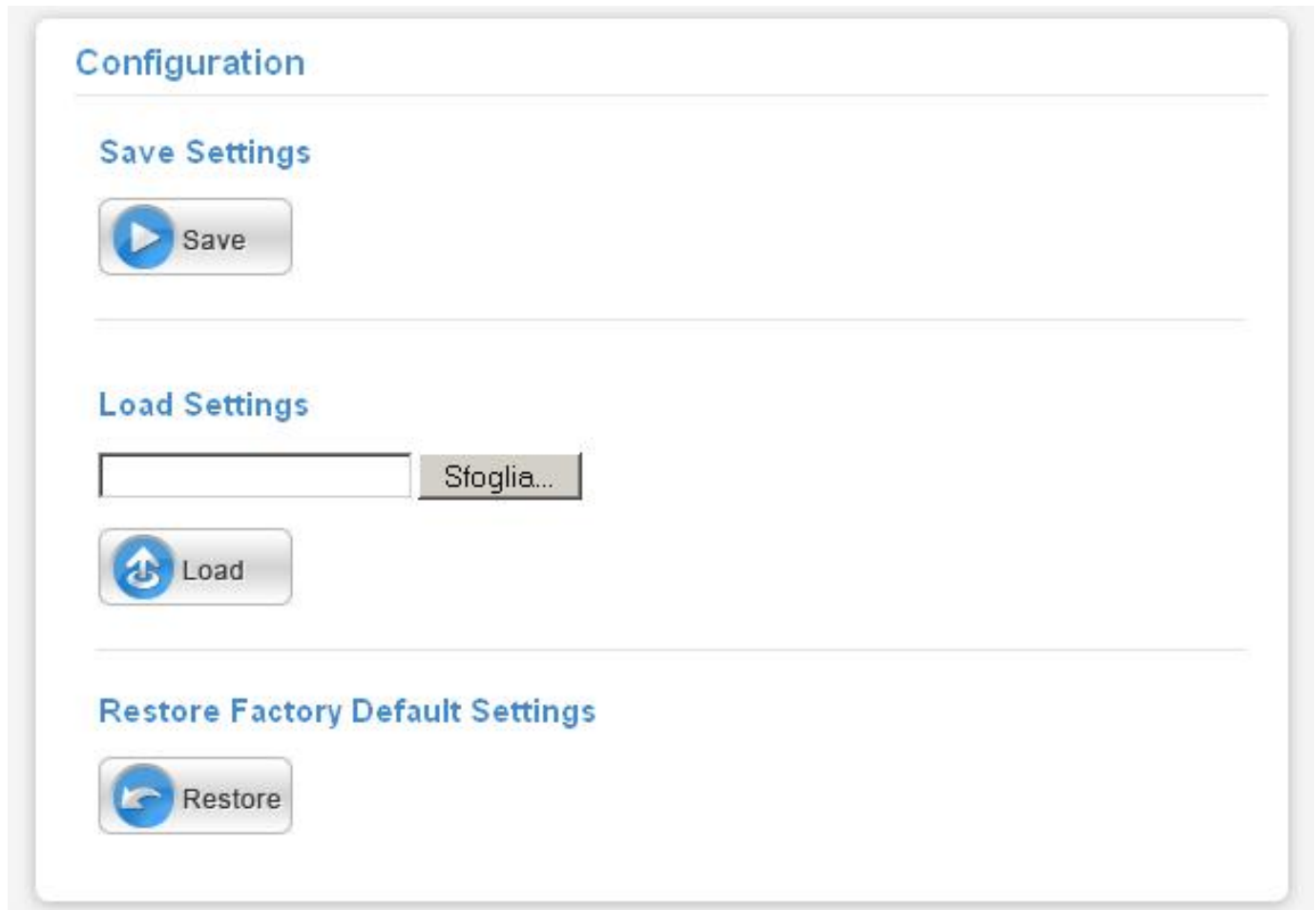
E' opportuno garantire, durante l'intera fase di upgrade, al Wireless Broadband Router l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.

Staccare il cavo WAN dal Router.

Non effettuare upgrade del firmware utilizzando l'interfaccia wireless ma solo quella wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.


3.8.9 Configuration

Il Wireless Broadband Router consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.

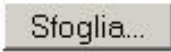



Configuration

Save Settings


 Save

Load Settings



 Load

Restore Factory Default Settings

 Restore

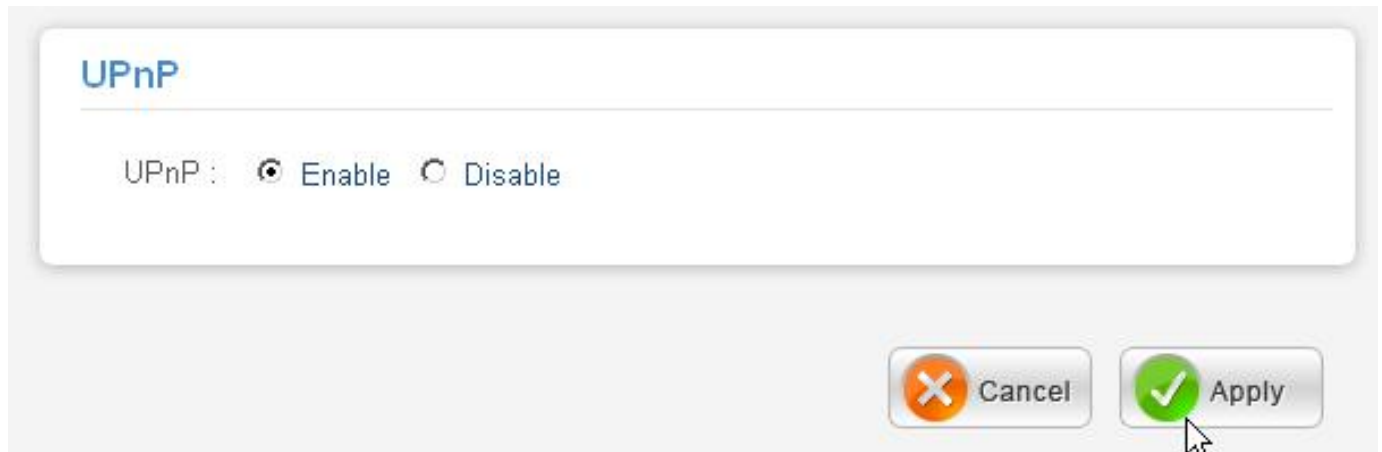
Per effettuare il Backup cliccare sul bottone **Save (in Save Settings)**. Non resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file config.BIN).

Per effettuare il Ripristino cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su **Load**.

Se per necessità si desidera reimpostare il router Wireless con la configurazione di default (perdendo tutti i settaggi inseriti) sarà sufficiente premere poi il tasto **Restore**. Il Router effettuerà un reboot e caricherà i settaggi di default.

3.8.10 UPnP

Il Wireless Broadband Router è dotato di un supporto UPnP, al fine di garantire il più alto grado di compatibilità con qualsiasi software.



Selezionare la voce **Enable** per abilitare questa funzionalità.
Cliccare poi su **Apply** per confermare l'operazione.

3.8.11 Ping Test

Il Wireless Broadband Router è dotato di un utility in grado di effettuare un ping test verso un indirizzo IP (o un host) specificato, al fine di verificare la connettività del prodotto.



Inserire l'indirizzo IP o l'Host Name verso cui effettuare una Echo Request.
Cliccare poi su **Ping** per effettuare l'operazione; verrà restituito l'esito del Ping Test.

3.8.12 Remote Management

In queste sezioni è possibile configurare le modalità con cui il dispositivo viene controllato da remoto.

Remote Management

HTTP

Enable Disable

Port :

Remote IP Range : From To

Allow to Ping WAN port

Enable Disable

Remote IP Range : From To

Gaming mode : Enabled Disabled

PPTP : Enabled Disabled

IPSec : Enabled Disabled

IDENT : Stealth Closed

HTTP: Consente l'accesso HTTP da remoto.

- **Enable:** per abilitare tale funzionalità
- **Port:** permette di scegliere la porta tramite cui configurare il dispositivo.
- **Remote IP Range:** consente di introdurre il range di IP da cui si effettua la configurazione remota.



Allow to PING WAN Port: Consente di bloccare/permittere il ping sulla porta WAN.

- **Enable:** per abilitare tale funzionalità (cioè permette il Ping).
- **Remote IP Range:** consente di introdurre il range di IP permesso da cui si effettua il Ping. Lasciando l'asterisco tutti gli IP sono permessi.

Gaming Mode: Qualora vengano riscontrati problemi nel gioco online o nell'uso di talune applicazioni è possibile risolvere i problemi attivando tale funzionalità. Quando non si usano tali applicazioni è consigliato disabilitare tale funzionalità.

PPTP: Spuntare questa funzione per abilitare la funzione di VPN PPTP Pass-Through.

IPSec: Spuntare questa funzione per abilitare la funzione di VPN IPSec Pass-Through.

IDENT: Permette all'utente di impostare la porta 113 in modalità Stealth..

APPENDICE A: Risoluzione dei problemi

Questo capitolo illustra come identificare e risolvere eventuali problemi sul Wireless Broadband Router.

A.1 LEDs

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED PWR non si accende

Steps	Azione Correttiva
1	Accertarsi che l'alimentatore sia connesso al Wireless Broadband Router e alla rete elettrica. Utilizzare unicamente l'alimentatore fornito a corredo.
2	Verificare che l'alimentatore sia connesso ad una presa elettrica attiva e in grado di fornire la tensione necessaria al funzionamento del prodotto.
3	Accertarsi che il Plug dell'alimentatore sia correttamente inserito.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra il Wireless Broadband Router e il PC o lo Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.3 LED WLAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Effettuare un reset ed attendere una cinquantina di secondi (tempo di reinizializzazione del modulo WLAN)
2	Eventualmente staccare il cavo di alimentazione e reinsertirlo.

A.2 Configurazione WEB

Non è possibile accedere all'interfaccia Web di configurazione.

Steps	Azione correttiva
1	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del Wireless Broadband Router (192.168.1.1).
2	Effettuare un reset del dispositivo.

Le schermate di configurazione Web non vengono visualizzate correttamente..

Steps	Azione correttiva
1	Accertarsi di utilizzare Internet Explorer 5 o una versione successiva.
2	Eliminare i files temporanei di Internet ed eseguire un nuovo login.

A.3 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, sarà necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante " Reset " presente nel pannello posteriore del prodotto per una decina secondi, il Wireless Broadband Router riporterà tutte le impostazioni ai valori iniziali (il tasto WLAN si spegnerà per indicare l'avvenuto reset, ricomincerà poi il caricamento di tutti i moduli necessari al funzionamento dell'apparato).
2	I parametri di default per l'accesso alla configurazione del Wireless Broadband Router sono: Username: admin Password: admin IP:192.168.1.1

	Canale=6 Sicurezza=Disabilitata SSSID=Default
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.4 Amministrazione remota

Non è possibile amministrare il Wireless Broadband Router da remoto.

Steps	Azione correttiva
1	Assicurarsi di aver abilitato la funzionalità Remote Management.
2	Assicurarsi che l'IP della macchina da cui si effettua il controllo remoto sia nel range di IP permessi(Management-Remote Management).
	

A.5 Domande Generali

Domanda	Posso avviare un' applicazione da un computer remoto presente sulla rete wireless?
----------------	--

Risposta	Questo dipende direttamente dall'applicazione stessa, se è stata progettata per lavorare in rete (non fa differenza che sia wireless o cablata) non ci sarà alcun problema.
-----------------	---

Domanda	Posso giocare in rete con gli altri computer presenti sulla WLAN?
----------------	---

Risposta	Sì, se il gioco è dotato di funzionalità multiplayer in rete.
-----------------	---

Domanda	Cos'è lo Spread Spectrum?
----------------	---------------------------

Risposta	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.
-----------------	---

Domanda	Cosa sono DSSS e FHSS?
----------------	------------------------

Risposta	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHSS (Frequency Hopping Spread Spectrum): è una tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.
-----------------	---

Domanda	Le informazioni inviate via wireless possono essere intercettate?
----------------	---

Risposta	Il Wireless Broadband Router offre funzionalità di crittografia WEP fino a 128 bit, ciò provvede a rendere sicure le trasmissioni dati wireless. L'utilizzo del WPA rende ancora più sicura la trasmissione wireless.
-----------------	---

Domanda	Cosa è il WEP?
Risposta	WEP è la sigla di Wired Equivalent Privacy, un protocollo di sicurezza per le reti locali senza fili (WLAN) definito dallo standard 802.11b.
Domanda	Cosa è la modalità Infrastructure?
Risposta	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point e/o Wireless Broadband Router.
Domanda	Cosa è il Roaming?
Risposta	Il Roaming è la capacità di un utente che possiede un computer portatile di comunicare senza interruzioni mentre si muove liberamente all'interno di una rete wireless la cui estensione è stata incrementata grazie all'utilizzo di più access point.
Domanda	Cosa è la banda ISM?
Risposta	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.
Domanda	Cosa è lo standard IEEE 802.11g ?
Risposta	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.
Domanda	Che cos'è il WDS?
Risposta	Il WDS (Wireless Distribution System) è la tecnologia che permette ad un Access Point di svolgere contemporaneamente la funzionalità di AP e di Repeater del segnale. Risulta essere la soluzione ottimale per estendere la copertura di una wireless LAN in ambienti dove non è assolutamente possibile stendere cavi. Può essere utile per raggiungere relocalizioni remote. Va osservato che l'uso di un repeater ha un forte impatto sulle

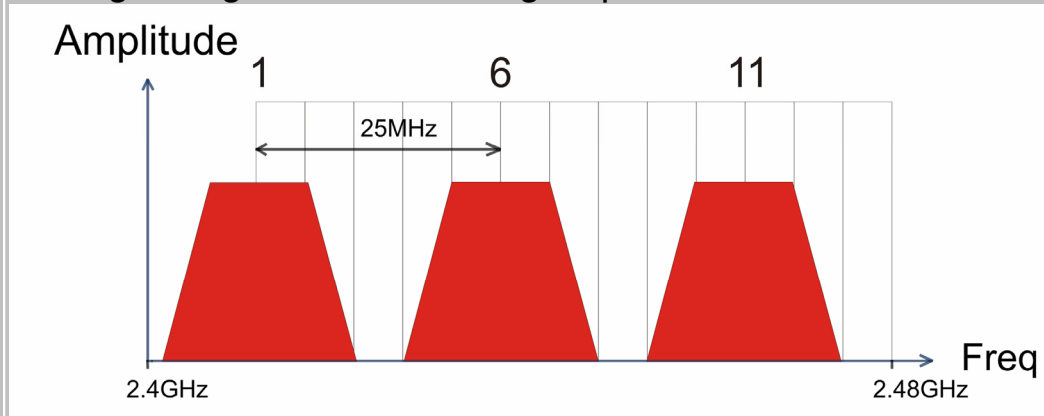
prestazioni dei client wireless ad esso collegati.
Il dispositivo in questione non supporta tale caratteristica.

Domanda Perché quando uso un Repeater le prestazioni dei client ad esso collegati calano drasticamente?

Risposta Le comunicazioni Wireless avvengono in modalità Half-Duplex pertanto ogni apparato può funzionare o in Trasmissione o in Ricezione.
Quando i Client connessi al Repeat (non ha logica e si appoggia sempre al Router) scambiano informazioni con la rete wired remota le prestazioni vengono pesantemente ridotte. I client Wireless devono prima inviare i dati al Repeat, questo a sua volta li invia al Router che li invia poi (tramite la connessione Wired) al client cablato. Appare evidente che le prestazioni avranno un picco (si aggiunge anche del traffico accessorio di gestione) inferiore della metà rispetto al caso in cui il client wireless sia linkato direttamente al Router.

Domanda Perché 2 AP benché utilizzino differenti canali interferiscono tra di loro?

Risposta Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili.
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).
L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
Il disegno seguente illustra meglio quanto detto:



Sino a 3 AP possono coesistere senza overlapping.
E' opportuno prestare attenzione all'assegnazione dei canali.

Domanda	I client IEEE802.11b funzionano con AP IEEE802.11g?
Risposta	<p>Senza alcun dubbio è possibile utilizzare client IEEE802.11b con AP IEEE802.11g. In questo caso si crea una WLAN ibrida.</p> <p>Le prestazioni ottenibili dai client IEEE802.11g risultano essere di gran lunga peggiori in una rete ibrida che non in una WLAN con solo apparati IEEE802.11g.</p> <p>Il consiglio è quello di migrare l'intera WLAN verso client IEEE802.11g.</p> <p>Vedere modalità Nitro GT™</p>

Domanda	Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?
Risposta	<p>Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze.</p> <p>Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi.</p> <p>In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.</p>

Domanda	Caratteristiche dell'Antenna?
Risposta	<p>Scegliere attentamente l'antenna adatta alle proprie esigenze, rivolgendosi a personale qualificato richiedendo:</p> <ul style="list-style-type: none"> • connettore tipo Reverse SMA, • compatibile con 802.11 standard (2.4Ghz) • 50 Ohm di impedenza <p>Si invita al rispetto delle normative vigenti (20dBm max)</p>

Domanda	Cos'è la ricezione in Diversity?
Risposta	<p>La propagazione elettromagnetica in un ambiente chiuso (o indoor) genera innumerevoli riflessioni dovute a cambiamenti di densità nel materiale attraversato.</p> <p>Queste riflessioni possono generare, soprattutto in ambienti interni pericolosi fenomeni:</p> <ul style="list-style-type: none"> • Cammini multipli: dovuti all'arrivo (sul ricevitore ad esempio) di segnali diretti e riflessi.

	<ul style="list-style-type: none"> • Forti attenuazioni: dovuti all'attraversamento di materiali diversi <p>Questo fenomeno è controllabile utilizzando antenne direttive o utilizzando 2 antenne in ricezione (cosiddetta diversity). Quando il dispositivo ricevente è colpito dal segnale controlla quale delle 2 antenne stia ricevendo il miglior rapporto segnale/rumore e utilizza quest'ultima. Si utilizzano in sostanza 2 punti spaziali diversi per effettuare un miglior campionamento del segnale ricevuto.</p>
--	---

Domanda	Posso utilizzare un cavo per collocare l'Antenna esterna in una miglior posizione?
Risposta	<p>Certo, non bisogna sottovalutare anche la collocazione geometrica dell'antenna.</p> <p>E' però altresì importante conoscere che ogni cavo introduce un'attenuazione espressa (in dB/m).</p> <p>Un cavo molto lungo può vanificare l'effetto positivo generato da un'antenna con alto guadagno.</p>

Domanda	Quali Antenne posso utilizzare per ampliare la copertura del dispositivo?
Risposta	<p>Vengono elencati i codici disponibili a listino Atlantis Land.</p> <p>A02-ANT0501 Antenna isotropica con guadagno di 5 dBi</p> <p>A02-ANT0601 Antenna isotropica con guadagno di 6 dBi</p> <p>A02-ANT06D03 Antenna direttiva con guadagno di 6 dBi</p> <p>Si raccomanda sempre il rispetto delle norme vigenti in merito ai limiti sulla propagazione elettromagnetica.</p>

Domanda	Introduzione ai decibel (cos'è)?
Risposta	<p>Il deciBel è un'unità misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una</p>

misura compressa e non lineare.
L'equazione canonica è la seguente: $dB = 10 \log_{10} (P_2 / P_1)$. Dove P_1 è la misura riferimento e P_2 è la misura istantanea.

Domanda	Introduzione al dBm (cos'è)?																																																						
Risposta	<p>Definiamo il $dBm = 10 \log_{10} (P_2 / P_1)$, dove $P_1 = 1$ milliWatt (mW).</p> <p>E' possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm.</p> <p>Nella tabella seguente è riportata l'equivalenza per i valori più comuni (utilizzare la formula di sopra per valori non in tabella):</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>dBm</th> <th>Watt</th> <th>note</th> </tr> </thead> <tbody> <tr><td>0</td><td>1 mW</td><td></td></tr> <tr><td>3</td><td>2 mW</td><td></td></tr> <tr><td>6</td><td>4 mW</td><td></td></tr> <tr><td>9</td><td>8 mW</td><td></td></tr> <tr><td>10</td><td>10 mW</td><td></td></tr> <tr><td>12</td><td>15,8 mW</td><td></td></tr> <tr><td>13</td><td>20 mW</td><td></td></tr> <tr><td>14</td><td>25 mW</td><td></td></tr> <tr><td>15</td><td>32 mW</td><td></td></tr> <tr><td>16</td><td>40 mW</td><td></td></tr> <tr><td>17</td><td>50 mW</td><td></td></tr> <tr><td>18</td><td>63 mW</td><td></td></tr> <tr><td>19</td><td>79 mW</td><td></td></tr> <tr><td>20</td><td>100 mW</td><td>Massima Potenza utilizzabile per WLAN a 2.4Ghz</td></tr> <tr><td>23</td><td>200 mW</td><td></td></tr> <tr><td>26</td><td>400 mW</td><td></td></tr> <tr><td>29</td><td>800 mW</td><td></td></tr> </tbody> </table>	dBm	Watt	note	0	1 mW		3	2 mW		6	4 mW		9	8 mW		10	10 mW		12	15,8 mW		13	20 mW		14	25 mW		15	32 mW		16	40 mW		17	50 mW		18	63 mW		19	79 mW		20	100 mW	Massima Potenza utilizzabile per WLAN a 2.4Ghz	23	200 mW		26	400 mW		29	800 mW	
dBm	Watt	note																																																					
0	1 mW																																																						
3	2 mW																																																						
6	4 mW																																																						
9	8 mW																																																						
10	10 mW																																																						
12	15,8 mW																																																						
13	20 mW																																																						
14	25 mW																																																						
15	32 mW																																																						
16	40 mW																																																						
17	50 mW																																																						
18	63 mW																																																						
19	79 mW																																																						
20	100 mW	Massima Potenza utilizzabile per WLAN a 2.4Ghz																																																					
23	200 mW																																																						
26	400 mW																																																						
29	800 mW																																																						

Domanda	Cos' è un'antenna Isotropica?
Risposta	<p>Antenna che irraggia senza prediligere alcuna specifica direzione nello spazio circostante. E' possibile fare un paragone con l'irraggiamento luminoso di una lampadina che avviene uniformemente in tutto lo spazio circostante.</p> <p>Effettuando una rilevazione della densità superficiale di</p>

potenza su una superficie sferica, il cui centro è posto sull'antenna, questa è uniforme.
Tale valore, espresso in $[W]/[m^2]$, è legato all'inverso del quadrato della distanza tra il punto in cui si effettua la rilevazione e la sorgente (punto da cui l'antenna irradia il segnale).

Domanda	Cos' è un'antenna Direttiva(con un certo guadagno)?
Risposta	Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza.

Domanda	Cos' è il dBi?
Risposta	Il guadagno di un'antenna è definito come il rapporto fra la densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P_2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza. Definiamo il $dBi = 10 \log_{10} (P_2 / P_{isotropica})$, $dBm = 10 \log_{10} (Potenza / 1mW)$

Domanda	Confronto fra Antenne direttive ed isotropiche			
Risposta	In tabella è possibile osservare i vantaggi e gli svantaggi di ciascun tipo di antenna:			
	Tipologia	Caratteristiche	Copertura	Installazione
	Isotrope	Coprono un angolo di 360°	Copertura relativamente bassa	Facili da installare
	Direttive	Proiettano un cono relativamente ristretto	Copertura anche molto elevata	Richiedono un'attenta installazione

Domanda	La Legge
Risposta	<p>L'EIRP è la Potenza Isotropica Effettiva Irradiata (Isotropica significa 'in ogni direzione') ed indica essenzialmente la potenza che effettivamente 'esce' dall'antenna.</p> <p>L'EIRP è sempre limitato per legge ed in Italia per i 2.4GHz questo limite è di 20dBm, pari a 100mW.</p> <p>Questo valore è la somma di:</p> <ul style="list-style-type: none"> • potenza al connettore dell'Access Point/ Wireless Broadband Router • guadagno d'antenna espresso in dBi. <p>La legge non fa distinzioni sul tipo di antenna utilizzato</p> <p>Questa potenza è la somma della potenza irradiabile e del guadagno dell'antenna</p> <p>Quindi per le antenne direttive la misurazione va effettuata nel cono di maggior irradiazione</p> <p>E' possibile accedere al sito del ministero delle comunicazioni (www.comunicazioni.it) per scaricare la modulistica e l'intera legge.</p>

Domanda	Attenuazione di Spazio Libero?																				
Risposta	<p>E' possibile utilizzare la formula di Friis per avere (in dB) l'attenuazione di spazio libero:</p> $\text{Attenuazione(dB)} = 92,45 + 20 \cdot \text{Log}_{10} F + 20 \text{Log}_{10} D$ <p>D=espressa in Km F=frequenza in GHz</p> <p>Per avere un'idea nella tabella sottostante sono stati inserite le distanze più comuni (F=2.450GHz):</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Distanza</th> <th>Attenuazione in dB</th> </tr> </thead> <tbody> <tr><td>100m</td><td>80,2</td></tr> <tr><td>150m</td><td>83,7</td></tr> <tr><td>200m</td><td>86,2</td></tr> <tr><td>250m</td><td>88,2</td></tr> <tr><td>300m</td><td>89,7</td></tr> <tr><td>500m</td><td>94,2</td></tr> <tr><td>750m</td><td>97,7</td></tr> <tr><td>1000m</td><td>100,2</td></tr> <tr><td>1500m</td><td>103,7</td></tr> </tbody> </table>	Distanza	Attenuazione in dB	100m	80,2	150m	83,7	200m	86,2	250m	88,2	300m	89,7	500m	94,2	750m	97,7	1000m	100,2	1500m	103,7
Distanza	Attenuazione in dB																				
100m	80,2																				
150m	83,7																				
200m	86,2																				
250m	88,2																				
300m	89,7																				
500m	94,2																				
750m	97,7																				
1000m	100,2																				
1500m	103,7																				

2000m

106,3

Partendo dal calcolo dell'attenuazione per una certa distanza è possibile utilizzare (per evitare calcoli) i seguenti accorgimenti:

- Si ricorda che al raddoppio della distanza è necessario aggiungere 6dB all'attenuazione.
- Si ricorda che quando si dimezza la distanza è necessario sottrarre 6dB all'attenuazione.

Appendice B: Come Avviene la comunicazione Wireless

La comunicazione in una WLAN avviene tramite onde radio che hanno una frequenza compresa tra 2.4Ghz e 2.48Ghz. Vengono dunque utilizzati circa 80Mhz di banda ISM (è una banda libera per applicazioni industriali, scientifiche e mediche).

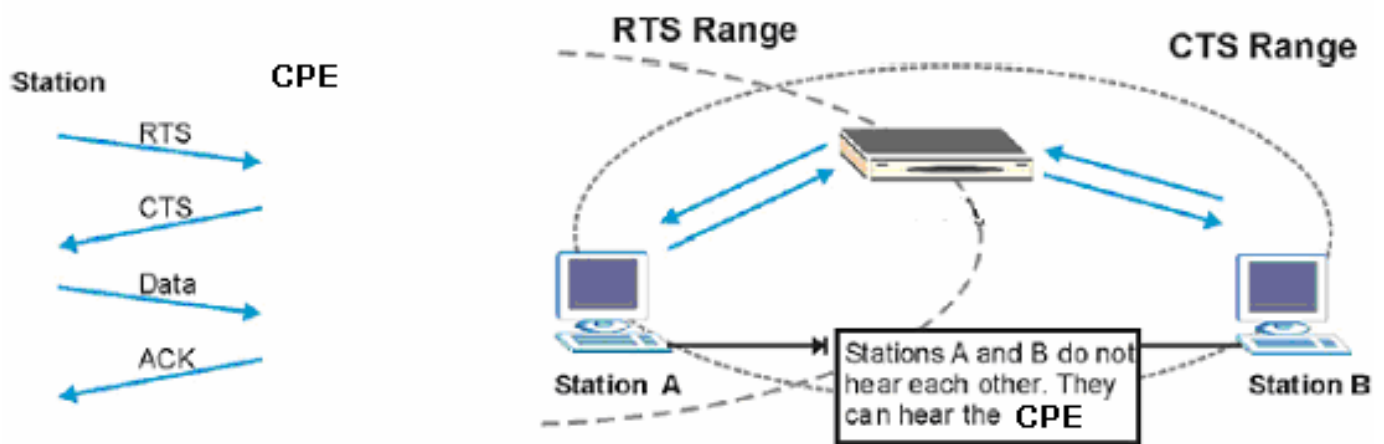
La trasmissione avviene dunque utilizzando un mezzo condiviso e possono pertanto sorgere delle collisioni durante l'accesso da parte dei client wireless.

Il protocollo CSMA/CA ("carrier sense multiple access with collision avoidance") è responsabile di garantire una politica di accesso corretta al mezzo, limitando al massimo il numero di collisioni.

Un client(o nodo), infatti, prima di inviare un pacchetto dati si mette in ascolto e, rilevato il canale libero, invia i dati.

RTS/CTS

Quando due stazioni Wireless sono all'interno del range dello stesso Wireless Broadband Router ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.



La stazione A invia dei dati all'AP ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono al Wireless Broadband Router.

Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS al Wireless Broadband Router per ottenere il permesso ad iniziare. Il Wireless Broadband

Router invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.

A questo punto, il nodo ricevente, dopo aver controllato l'integrità dei dati ricevuti (a tal fine viene utilizzato una sorta di CRC) invia un messaggio di ACK per informare il trasmittente dell'avvenuta corretta ricezione del pacchetto.



L'utilizzo di questo protocollo unito all'invio di ACK (segnalazione di corretta ricezione di un frame) di corretta ricezione ed al traffico di gestione e controllo comporta un importante overhead che riduce, in maniera sensibile, il throughput massimo ottenibile.

Canali

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b/g è suddiviso in "canali". Il numero di canali disponibili dipende dall'area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point/ Wireless Broadband Router vicini.

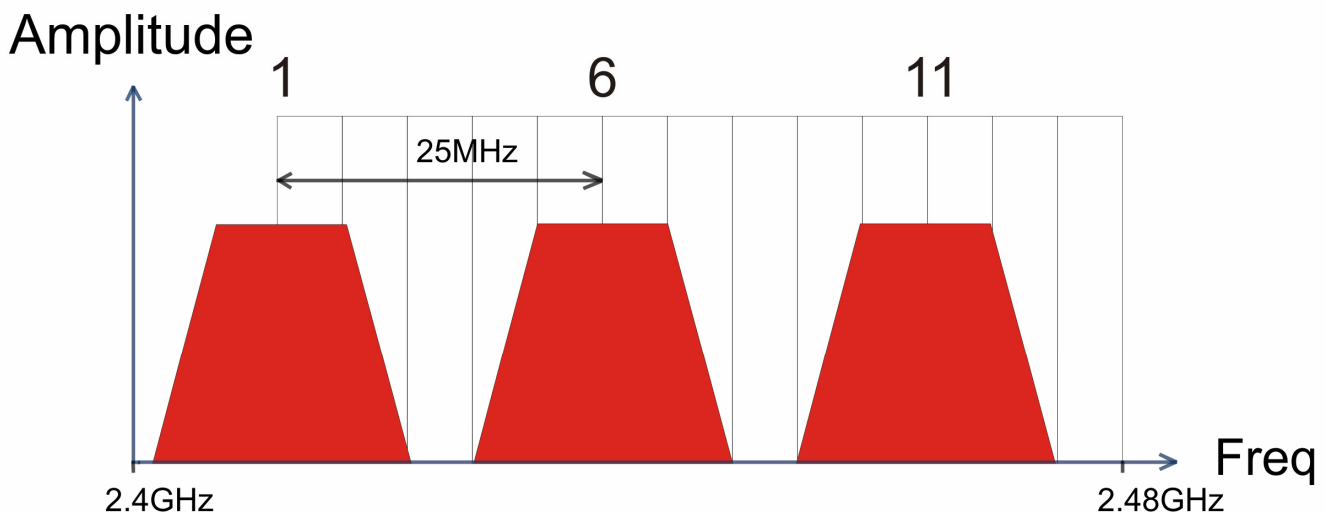
L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".

E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).



Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili.

Il disegno seguente illustra meglio quanto detto:



Utilizzando un quarto AP questo andrebbe a creare fenomeni di overlapping (sovrapposizione spettrale) generando un drastico deterioramento delle prestazioni.

Modalità Operative

Lo standard integra 2 differenti modalità operative:

- **Infrastructure:** in questa modalità i differenti client si contendono il mezzo radio e quindi ai servizi messi a disposizione dalla rete. La gestione delle contese è affidata ad un'entità centralizzata che prende il nome di Punto d'Accesso. Con l'uso di algoritmi di sicurezza l'AP può anche essere responsabile dell'autenticazione dei client e cifratura del traffico.
- **Ad Hoc:** in questa modalità non è presente un AP ma soltanto una moltitudine di client che devono essere configurati con lo stesso SSSID, lo stesso canale, in modalità Ad-Hoc e con la stessa chiave WEP.

Appendice C: Sicurezza nel Wireless

Per la natura stessa delle reti wireless tutta una nuova serie di considerazioni sulla sicurezza vanno affrontate. Il segnale radio può infatti essere intercettato da terzi non autorizzati che potrebbero cercare di estrarne informazioni preziose.

Sino ad oggi la sicurezza nelle reti WLAN è stata garantita dal protocollo WEP (Wired Equivalent Privacy) a 64/128. Purtroppo:

- le vulnerabilità WEP protocollo e la non facilità del contenimento del segnale wireless
- disattese aspettative di throughput

hanno generato, in taluni utenti, una certa diffidenza nei confronti della Tecnologia Wireless.

Per cercare di colmare alle lacune della sicurezza Wireless la IEEE sta sviluppando un nuovo standard, chiamato IEEE802.11i, che permetterà di rendere le reti wireless finalmente affidabili.

In attesa della ratifica di questo standard la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).

Come opera il WEP

Il segnale radio, come già evidenziato in precedenza, è di difficile contenimento e può pertanto essere intercettato da utenti non autorizzati (è sufficiente che abbiano un comune client wireless in standard IEEE802.11b/g).

Il protocollo WEP nasce per limitare questo fenomeno.

Nel dettaglio i servizi offerti dal WEP sono:

- autenticazione delle stazioni che accedono ai servizi di rete
- integrità dei dati trasmessi sul canale radio (nessun cambiamento è possibile senza che il sistema non se ne accorga)
- riservatezza dei dati trasmessi sul canale radio (nessuno può comprendere l'informazione contenuta nei pacchetti che sono cifrati con l'algoritmo RC4)

Le principali critiche mosse al WEP sono le seguenti:

- Una sola chiave segreta è utilizzata per l'autenticazione (di fatto non si autentica un client, al massimo si sa che il client appartiene al gruppo di utenti autorizzati)
- Un client che conosce la chiave può intercettare tutto il traffico scambiato dagli altri client wireless.
- La chiave di autenticazione è statica ed è usata anche per la cifratura (un attaccante può cercare di entrare nel sistema decifrando il traffico dati che contiene questa chiave)

- Debolezza nel modo con cui il WEP costruisce la chiave di cifratura (diversa ogni trama) coi cui l'RC4 cifra il messaggio
- Debole contro attacchi di integrità o che sfruttano la mancanza di autenticazione di ogni messaggio

Come opera il WPA (in modalità PSK e 802.11x)

In attesa della ratifica dello standard IEEE802.11i la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).

Le caratteristiche peculiari del WPA sono:

- Integrazione del TKIP (Temporal Key Integrity Protocol) per permettere il cambio della chiave e migliorare il controllo di integrità dei pacchetti
- Meccanismo avanzato per gestire l'autenticazione e il controllo degli accessi ai servizi di rete in modo centralizzato (802.11x tramite EAP, l'uso di TLS è obbligatorio)
- La chiave di autenticazione è diversa da quella utilizzata per la cifratura (che grazie al TKIP cambia continuamente)
- Permette l'autenticazione direttamente sull'AP (WPA-PSK)

Cosa prevede il futuro (WPA2)

Approvato di recente dalla Wi-Fi Alliance, il nuovo standard WPA2 è l'evoluzione del primo WPA (Wi-Fi Protected Access) che è oggi supportato dalla maggior parte degli apparati compatibili IEEE802.11g.

Lo standard WPA, richiesto prepotentemente dal mercato per porre fine alla debolezza intrinseca del WEP, ha purtroppo tratto dall'802.11i solo una parte delle specifiche.

Il nuovo WPA2 invece abbracciando pienamente l'IEEE802.11i ha necessariamente introdotto il supporto per l'Advanced Encryption Standard (AES), protocollo di cifratura utilizzato già da tempo nelle VPN IPSec.

I dispositivi WPA2 saranno compatibili con quelli WPA che però dovranno essere riaggiornati tramite il rilascio di nuovi firmware e/o driver. Il problema risiede nella capacità di calcolo (richiesta dall'AES) che rischierebbe di essere praticamente troppo elevata per gli apparati oggi in commercio.

Ogni sistema di cifratura dati è basato su password.

Queste possono essere lunghe, nel caso del WPA in PSK, da 8 sino a 63 caratteri.



Più lunga è la password e meno ha senso compiuto (usare caratteri alfanumerici, numeri e punteggiatura di ogni genere) più questa risulterà sicura.

Appendice D: Access Point o Router

Modalità Access Point

In questa modalità il Router è collegato alla vostra LAN tramite una delle 4 porte Fast Ethernet (e la porta WAN è inutilizzata).

In questo caso è necessario collocare il Wireless Router sulla stessa classe degli apparati cui è collegato.

Modalità Router (Con NAT abilitato)

Quando si implementa il Nat si isola di fatto la propria Lan dalla porta WAN (e quello cui questa è collegata). La Lan locale, se privata, deve avere gli indirizzi IP appartenenti ai seguenti blocchi (riservati dall'ente IANA per reti private).

CLASSE	IP Partenza	IP Finale	Subnet Mask
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

E' chiaramente raccomandato scegliere gli indirizzi della Lan appartenenti alla tabella di sopra (per ulteriori informazioni fare riferimento all'RFC 1597). Scegliendo dei blocchi pubblici potrebbero sorgere problemi di mancata visibilità di taluni siti internet.

Scenari più comuni:

- PC con IP appartenenti ad una classe privata, il cui default gateway è il Router Wireless che fa NAT. Può essere attivo o meno il DHCP (il Router prenderà sull'interfaccia WAN un indirizzo IP statico o dinamico, a seconda della configurazione). Il collegamento con l'ISP può essere uno qualsiasi tra quelli supportati (il default gateway del Router ADSL sarà dato automaticamente come i DNS in caso di PPPoE e PPPoA, dovranno essere inseriti in caso di altri protocolli come RFC1483/1577). In questo caso dunque una possibile configurazione della LAN sarebbe la seguente:

Host	Indirizzo IP	Maschera	Gateway	DNS
Router Lan IP	192.168.1.1	255.255.255.0		
PC A	192.168.1.2	255.255.255.0	192.168.1.1	Forniti ISP
PC B	192.168.1.3	255.255.255.0	192.168.1.1	Forniti

				ISP
PC C	192.168.1.4	255.255.255.0	192.168.1.1	Forniti ISP
PC X	192.168.1.n	255.255.255.0	192.168.1.1	Forniti ISP

In questo caso si è scelto di mantenere la rete 192.168.1.x e l'indirizzo IP (per il Wireless Broadband Router) di default. E' possibile in questo caso abilitare il DHCP server del Router (per assegnare ulteriori indirizzi IP, magari a PC portatili) ma bisogna prestare attenzione nello scegliere un pool di indirizzi compatibile (in questo caso bisognerà settare come IP starting 192.168.1.n+1, dove $n+1 < 254$).

E' comunque possibile cambiare la rete, avendo l'accortezza di sceglierla tra quelle riservata dallo IANA a tale utilizzo.

- PC con IP appartenenti ad una classe pubblica, in questo caso tutti i PC della Lan sono raggiungibili da Internet e l'interfaccia Lan del Router ha anch'essa un indirizzo IP pubblico. Il default gateway dei PC è l'indirizzo IP della Lan del Router che avrà chiaramente il NAT disabilitato. L'interfaccia WAN del Router prenderà un IP che può essere pubblico o privato, l'ISP fornirà comunque l'indirizzo del default gateway del Wireless Broadband Router assieme alla subnet mask. Questo scenario è tipico, ma non esclusivo, con l'uso del protocollo RFC 1483 o RFC 1577. Come già accennato è possibile che l'ISP utilizzi una punto-punto composta da indirizzi IP che possono essere pubblici o privati.

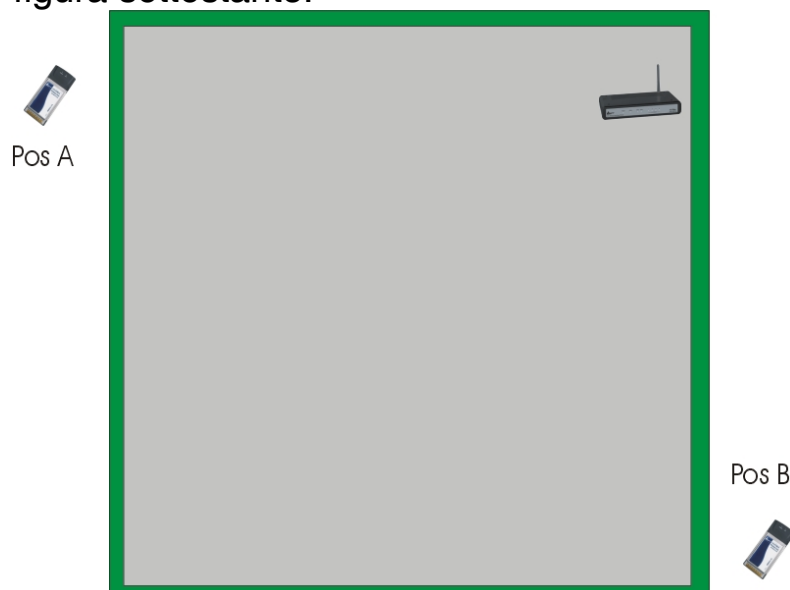
Appendice E: Copertura

Considerazioni Generali

In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire diverse decine di metri. E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine.

Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.
- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E' bene prendere in considerazione questo fatto.
- Allontanare l'AP Wireless da ogni altro dispositivo che produca emissioni RF.
- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless AP col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante). Si veda la figura sottostante:

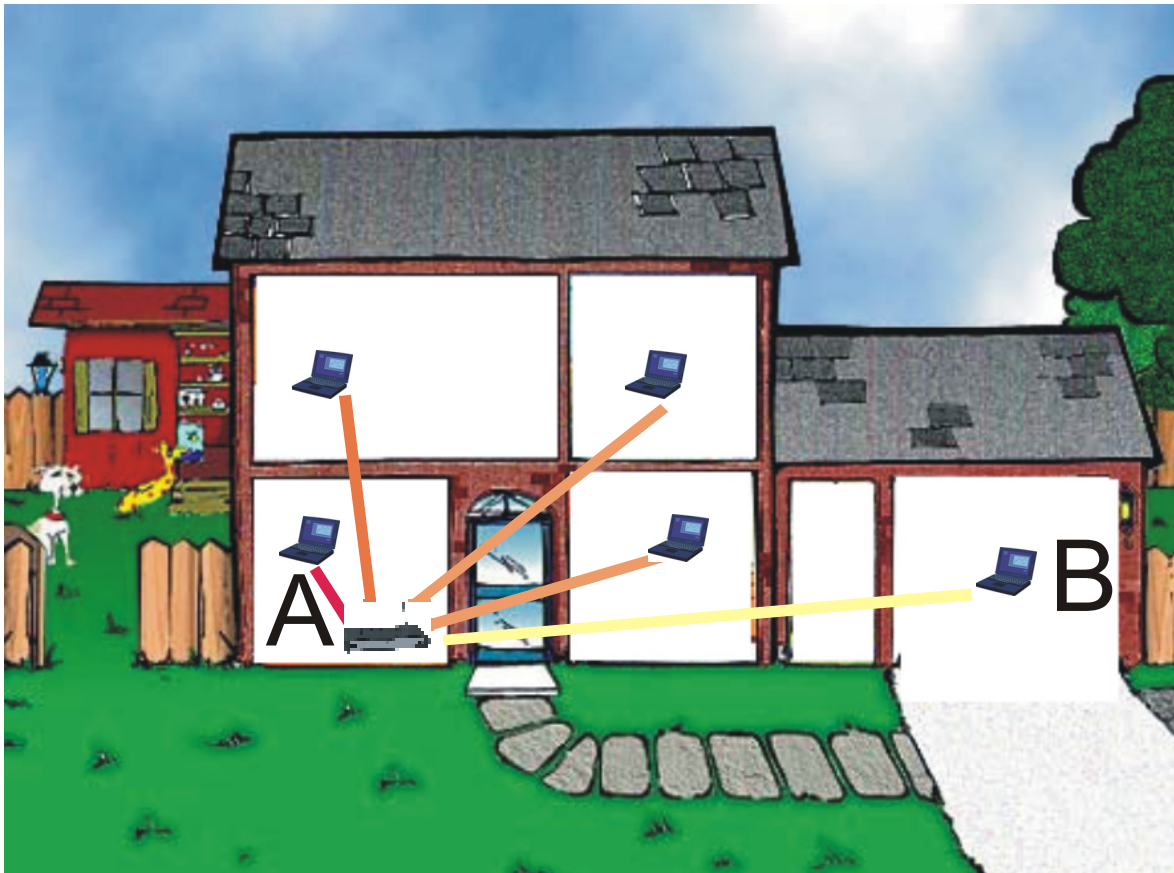


Il Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A, benché la distanza effettiva

dall'AP sia quasi identica nei 2 casi. E' sufficiente collocare il Wireless AP al centro del locale per migliorare decisamente le prestazioni del client B.

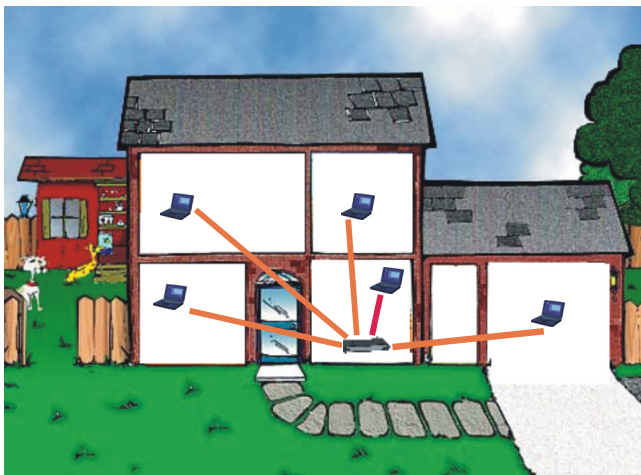
Dove installare un AP

Immaginiamo di avere un'installazione come quella in figura.



Sicuramente Client in posizione B avrà un'enorme attenuazione e peggiori prestazioni che non il client in posizione A.

E' sufficiente collocare il Wireless Router/AP al centro della rete per migliorare decisamente le prestazioni di entrambi i client B.

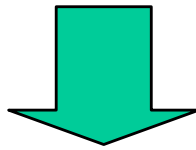


Si è operato sulla diminuzione 2 fattori:

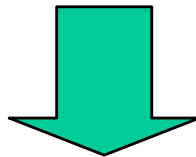
- Distanza media
- Sezioni di muro attraversate

E' decisamente meglio avere una rete i cui client abbiano un link mediamente buono che non una rete con taluni client con link eccellente ed altri con link molto scarso.

La stazione lontana, che generalmente trasmette con un data rate più basso, tende a consumare un «airtime» elevato.



L'AP ha meno tempo da dedicare a client più vicini e più veloci.



Prestazioni complessivi peggiori.

APPENDICE F: Considerazioni sulla Salute

Quando un organismo è immerso in un campo elettromagnetico avviene un'interazione nota come "effetto biologico". Non bisogna necessariamente associare all'"effetto biologico" un danno. Il problema può sorgere quando tale effetto supera la capacità di compensazione dell'organismo.

E' opportuno considerare che il livello di emissioni di un dispositivo wireless conforme alle direttive stabilite dall'IEEE (Institute of Electrical and Electronic Engineers) è notevolmente inferiore all'emissione generata da dispositivi di uso comune.

Un comune terminale GSM emette infatti una potenza che può arrivare e superare i 600mw, mentre un apparato UMTS emette una potenza del 20% inferiore.

A titolo di confronto un apparato Wireless difficilmente supera, in condizione di uso normale, i 17 dBm (circa 50mW) essendo di fatto oltre un ordine di grandezza inferiore.

Già queste considerazioni puramente energetiche dovrebbero tranquillizzare circa ogni eventuale dubbio.

Va inoltre considerato che l'uso del cellulare avviene ad una distanza tipica di qualche centimetro e dunque, essendo l'antenna di tipo isotropica, metà della potenza trasmessa attraversa la testa dell'utilizzatore e crea un effetto "riscaldamento" avvertibile soprattutto nei tessuti superficiali.

Nel caso di un apparato wireless possono presentarsi 2 casi diversi:

- Antenna isotropica: va considerato l'angolo solido con cui questa viene vista (generalmente qualche grado)
- Antenna direttiva: emette potenza solo nella zona di direttività

In entrambi i casi l'energia che arriva all'utilizzatore va da una frazione di quella trasmessa (e non la metà come nel caso del cellulare) sino ad arrivare a zero nel caso di antenna direttiva.

In tabella un grafico comparativo di quanto sin qui detto:

Apparato	Potenza Emessa	Angolo di Visuale	Potenza Effettiva
Wireless IEEE802.11b/g	50mW	1/15	<5mW
Cellulare GSM	600mW	1/2	Circa 300mW
Cellulare UMTS	500mW	1/2	Circa 250mW



Il Decreto del 20 Giugno 1995, n.458 (Legge Cautelativa dello Stato) impone di usare il telefonino tenendo l'antenna ad almeno 20cm da qualsiasi parte del proprio corpo.



Ad oggi, tutti gli studi effettuati hanno concluso che non esistono effetti termico-biologici pericolosi, a patto di rispettare le norme ETSI sull'emissione.

APPENDICE G: Packet Filter

Il Wireless Router dispone di un sofisticato Packet Filter col quale riesce ad esaminare tutto il traffico che lo attraversa. In questo modo è possibile, conoscendo le caratteristiche dei pacchetti IP associati ai più comuni servizi, effettuare i filtraggi in maniera corretta. In questa appendice verranno evidenziate le varie modifiche subite da un pacchetto durante il percorso.

Condizioni di partenza:

- NAT attivo
- PCX della LAN con IP 192.168.1.X
- Router con LAN IP 192.168.1.254

Il caso da esaminare prevede una LAN in cui il PC con IP 192.168.1.X vuole visualizzare un sito WEB.

Vi sono 2 fasi: Risoluzione dell'URL (tale valore potrebbe essere recuperato in qualche cache o fornito da appositi programmi, ma per completezza verrà affrontato il caso più comune) e costruzione della connessione TCP col sito WEB.

Il primo pacchetto è inviato dal PC (con IP 192.168.1.X) verso il server DNS per chiedere la risoluzione dell'URL cercato.

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	C	
	Porta Destinazione	53	

Questo pacchetto uscente arriva al Wireless Router che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendo il suo IP Pubblico e lo inoltra al server DNS.

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	IP lato WAN del Router	
	IP Destinazione	IP del Server DNS	
	Pacchetto contenuto	Tipo UDP	U D
	Porta Provenienza	C	

	Porta Destinazione	53	P
--	--------------------	----	---

Arrivato al server DNS il pacchetto torna indietro, reindirizzato al Wireless Router (che ne aveva cambiato prima l'IP di provenienza). Sono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello UDP.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	IP del Server DNS	
	IP Destinazione	IP lato WAN del Router	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	53	
	Porta Destinazione	C	

Arrivato al Wireless Router il pacchetto viene riprocessato ed inviato al PC di provenienza.

	Direzione Pacchetto	Internet-Router[Entrante]	
IP	IP Provenienza	IP del Server DNS	
	IP Destinazione	192.168.1.X	
	Pacchetto contenuto	Tipo UDP	U D P
	Porta Provenienza	53	
	Porta Destinazione	C	

A questo punto, dal pacchetto UDP arrivato, il PC (con IP 192.168.1.X) ha risolto l'URL e conosce l'indirizzo IP associato. Inizia dunque la fase della costruzione della connessione TCP (il protocollo TCP infatti richiede la costruzione della connessione, al contrario di quello UDP).

	Direzione Pacchetto	PC-Router[Uscente]	
IP	IP Provenienza	192.168.1.X	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	T C
	Porta Provenienza	K	

	Porta Destinazione	80	P
--	--------------------	----	---

Questo pacchetto uscente arriva al Router che (essendo abilitato il NAT) ne cambia l'indirizzo di provenienza mettendovi il suo Pubblico e lo inoltra al server WEB.

	Direzione Pacchetto	Router-Internet[Uscente]	
IP	IP Provenienza	IP lato WAN del Router	
	IP Destinazione	IP URL	
	Pacchetto contenuto	Tipo TCP	T C P
	Porta Provenienza	K	
	Porta Destinazione	80	

Arrivato al server WEB il pacchetto torna indietro, reindirizzato al Wireless Router (che ne aveva cambiato prima l'IP di provenienza). Vengono invertiti sia a livello IP i campi IP prov con IP dest e sia le porte nel livello TCP.

	Direzione Pacchetto	Internet- Router [Entrante]	
IP	IP Provenienza	IP URL	
	IP Destinazione	IP lato WAN del Router	
	Pacchetto contenuto	Tipo TCP	T C P
	Porta Provenienza	80	
	Porta Destinazione	K	

Arrivato al Wireless Router il pacchetto viene riprocessato ed inviato all'IP di provenienza.

	Direzione Pacchetto	Router-PC[Entrante]	
IP	IP Provenienza	IP URL	
	IP Destinazione	192.168.1.X	
	Pacchetto contenuto	Tipo TCP	T C
	Porta Provenienza	80	



	Porta Destinazione	K	P
--	--------------------	---	---

E' stato evidenziato tanto il percorso dei pacchetti che le trasformazioni che questi subiscono. Nell'esempio di sopra si sono utilizzati dei parametri C e K. Sono dei numeri interi >1024 . Nei protocolli per porta quali TCP/UDP infatti il mittente parla ad una porta di destinazione (su cui è in ascolto il server) ed indica una porta (la porta di provenienza appunto) dove aspetta la risposta. Il pacchetto una volta ricevuto dal server viene reinviato al mittente sulla porta su cui questo aspetta la risposta (viene effettuata un'inversione a livello di porte).

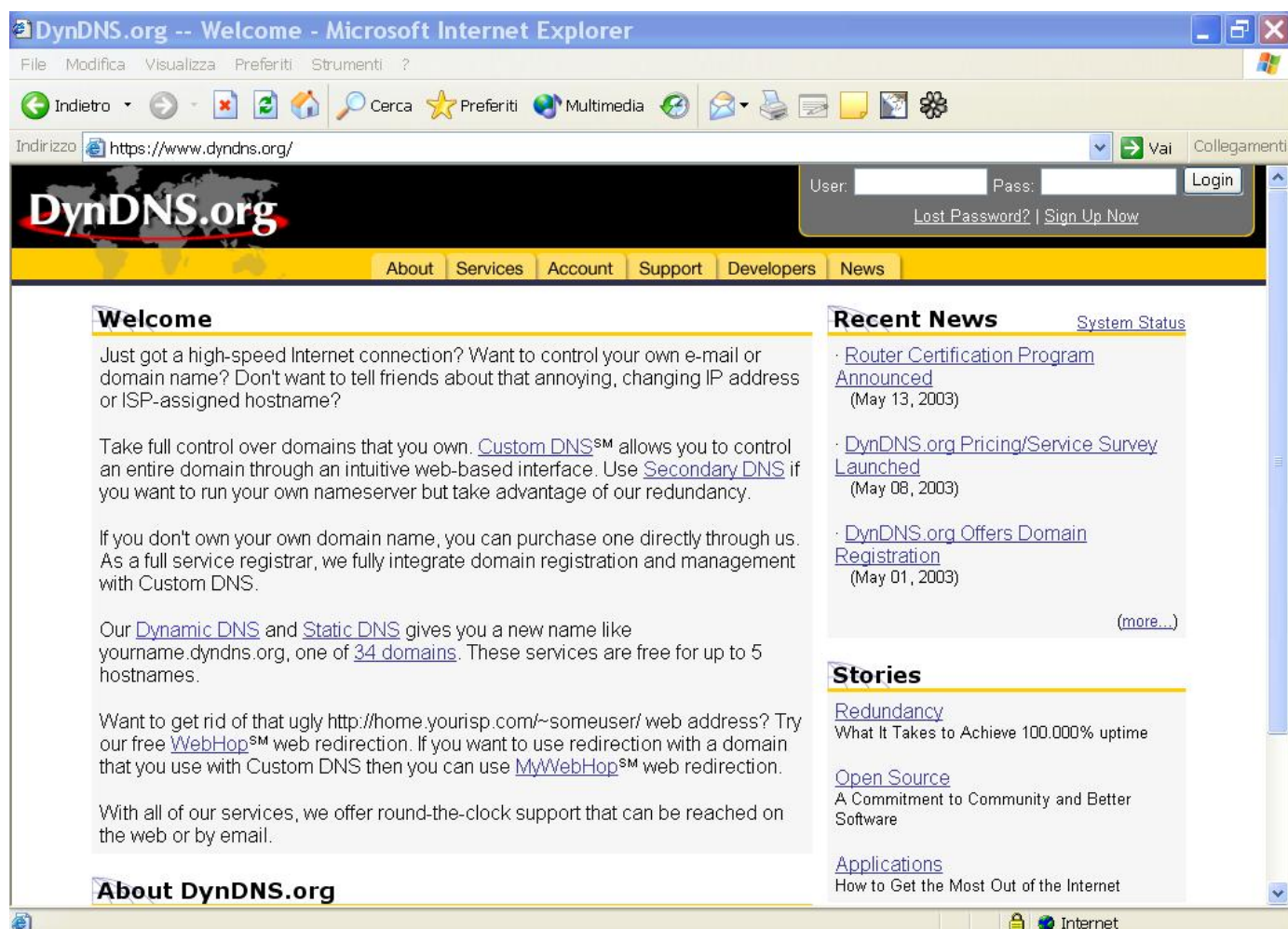
APPENDICE H: Dynamic DNS

Grazie all'adozione di questa features è possibile registrare un dominio pur se associato ad un IP dinamico. Ci sono una moltitudine di server DDNS che offrono gratuitamente questo tipo di servizio. E' sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che consentirà di raggiungere (da remoto) sempre il Router ADSL2+. E' possibile in questo modo effettuare facilmente configurazioni da remoto, ospitare un sito WEB o FTP.

Ogni qual volta che l'Adsl2+ VPN Router si riconnetterà, tramite il client incorporato, comunicherà al server DDNS il nuovo indirizzo IP. In questo modo chiunque dall'esterno conoscendo l'URL conoscerà anche l'indirizzo IP che in quel momento è stato assegnato all'Adsl2+ VPN Router.

Vediamo, nel dettaglio come effettuare una registrazione con il gestore DDNS forse più famoso.

Andare nel sito: www.dyndns.org, cliccare su Account.



DynDNS.org

User: Pass:
[Lost Password?](#) | [Sign Up Now](#)

[About](#) [Services](#) [Account](#) [Support](#) [Developers](#) [News](#)

Welcome

Just got a high-speed Internet connection? Want to control your own e-mail or domain name? Don't want to tell friends about that annoying, changing IP address or ISP-assigned hostname?

Take full control over domains that you own. [Custom DNSSM](#) allows you to control an entire domain through an intuitive web-based interface. Use [Secondary DNS](#) if you want to run your own nameserver but take advantage of our redundancy.

If you don't own your own domain name, you can purchase one directly through us. As a full service registrar, we fully integrate domain registration and management with Custom DNS.

Our [Dynamic DNS](#) and [Static DNS](#) gives you a new name like yourname.dyndns.org, one of [34 domains](#). These services are free for up to 5 hostnames.

Want to get rid of that ugly [http://home.yourisp.com/~someuser/](#) web address? Try our free [WebHopSM](#) web redirection. If you want to use redirection with a domain that you use with Custom DNS then you can use [MyWebHopSM](#) web redirection.

With all of our services, we offer round-the-clock support that can be reached on the web or by email.

Recent News

[Router Certification Program Announced](#)
(May 13, 2003)

[DynDNS.org Pricing/Service Survey Launched](#)
(May 08, 2003)

[DynDNS.org Offers Domain Registration](#)
(May 01, 2003)

[\(more...\)](#)

Stories

[Redundancy](#)
What It Takes to Achieve 100.000% uptime

[Open Source](#)
A Commitment to Community and Better Software

[Applications](#)
How to Get the Most Out of the Internet

About DynDNS.org



Effettuare la registrazione (cliccando su Create Account) inserendo: Username, Indirizzo Mail e Password.

Una mail di verifica registrazione sarà inviata all'indirizzo inserito. In questa mail sono contenute le istruzioni per proseguire la registrazione (è necessario confermare così il tutto entro 48 ore). Seguire le istruzioni contenute e compilare il form per terminare la fase di registrazione.

A questo punto tornare nel sito, andare su Services, evidenziare (nella parte sinistra) il menù Dynamic DNS e poi cliccare su Add Host.

Non resta che introdurre il Nome dell'host (evidenziare Enable WildCard) e scegliere il suffisso preferito e premere poi sul bottone Add Host per terminare.

APPENDICE I: Regolamentazione

Taluni paesi europei utilizzano una legislazione differente sull'utilizzo delle frequenze ISM. Consultare la tabella sottostante per conoscere i canali utilizzabili.

Canali	Country
1-11	USA/CANADA
1-13	ETSI(Europe)
10-11	Spain
10-13	France
14	MKK
1-14	Japan (MKKI Telecom)
3-9	Israel
5-13	Israel

APPENDICE J: Caratteristiche Tecniche

Standards	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.11g; IEEE 802.11b
Protocol	CSMA/CD
Radio Technology	IEEE 802.11g Orthogonal Frequency Division Modulation
Data Transfer Rate	802.11b: 1, 2, 5.5, 11Mbps (auto sense) 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps @802.11g(auto sense) Ethernet: 10Mbps (half duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps (full- duplex)
Topology	Star
Receiver Sensitivity	54Mbps: Typical -70dBm @ 10% PER (Packet Error Rate) 11Mbps: Typical -85dBm @ 8% PER (Packet Error Rate)
TX Power	13dBm typically @ 802.11g 13dBm typically @ 802.11b
Network Cables	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA-568 100-ohm STP (100 m) 100BASE-TX: 2-pair UTP Cat. 5 (100 m), EIA/TIA-568 100-ohm STP (100 m)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Security	64/128-bits WEP Encryption; WPA, WPA-PSK, WPA2. WPA2-PSK
Channels	1 ~ 11 channels (FCC); 1 ~ 13 channels (ETSI); 1 ~ 14 channels (MKK)
Number of Ports	LAN: 4 x 10/100Mbps Auto-MDIX Fast Ethernet port WAN: 1 x 10/100Mbps Auto-MDIX Fast Ethernet port
DC inputs	DC 7,5V / 1A
Power Consumption	7,5W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	147 x 115 x 35 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B

APPENDICE K: Supporto Offerto

Per ogni problema con il Wireless Broadband Router consultare questo manuale. Molti problemi potrebbero essere risolti cercando la soluzione del problema nell'APPENDICE A.

Per qualunque altro problema o dubbio è possibile contattare l'help desk telefonico (02/93907634) gratuito di Atlantis Land che fornirà assistenza da lunedì al giovedì dalle 9:00 alle 13:00 e dalle 14:00 alle 18:00. Il venerdì dalle 9:00 alle 13:00. E' possibile anche utilizzare il fax (02/93906161) la posta elettronica (info@atlantis-land.com oppure tecnici@atlantis-land.com).

Atlantis Land SpA

Viale De Gasperi 122

20017 Mazzo di Rho(MI)

Tel: 02/93907634(help desk)

Fax: 02/93906161

Email: info@atlantis-land.com oppure tecnici@atlantis-land.com (mettere nell'oggetto il codice del prodotto di cui si chiede assistenza)

WWW: <http://www.atlantiland.it> o www.atlantis-land.com